# Trgovina ljudima posredstvom interneta i tehnologije

## Detaljan izveštaj

courtesy translation / ljubazno prevođenje

**GRETA**
Grupa eksperata za borbu protiv trgovine ljudima

Prevod sufinansirala Evropska unija

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

# Trgovina ljudima posredstvom interneta i tehnologije

Detaljan izveštaj

Izveštaj pripremio
dr Paolo Kampana
vanredni profesor, Univerzitet u Kembridžu
Ujedinjeno Kraljevstvo

april 2022.

Savet Evrope

Izdanje na francuskom jeziku:
*La traite des êtres humains en ligne et facilitée par les technologies*

Prevod ovog dokumenta je pripremljen uz finansijsku podršku Evropske unije i Saveta Evrope. Sadržaj je isključiva odgovornost autora i ni u kom slučaju ne predstavlja zvanične stavove Evropske unije ni Saveta Evrope.



Sva ostala prepiska koja se odnosi na ovaj dokument treba da bude upućena Sekretarijatu Konvencije Saveta Evrope za borbu protiv trgovine ljudima trafficking@coe.int

Sve fotografije: Shutterstock

Uredničkа jedinica SPDP nije lektorisala ovu publikaciju radi ispravljanja tipografskih i gramatičkih grešaka.

# Sadržaj

# Skraćenice korišćene u tekstu

| | |
|---|---|
| AI: | Veštačka inteligencija |
| ASW: | Veb lokacija za usluge za odrasle |
| SE: | Savet Evrope |
| CID: | Odeljenje za krivične istrage |
| CSE: | Seksualna eksploatacija dece |
| CV: | Radna biografija |
| EAW: | Evropski nalog za hapšenje |
| EIO: | Evropski nalog za istragu |
| EJN: | Evropska pravosudna mreža |
| EU: | Evropska unija |
| BDP: | Bruto domaći proizvod |
| GDPR: | Opšta uredba o zaštiti podataka o ličnosti |
| GRETA: | Grupa eksperata Saveta Evrope za borbu protiv trgovine ljudima |
| HDD: | Čvrsti disk |
| ZIT: | Zajednički istražni tim |
| IKT: | Informaciono-komunikacione tehnologije |
| ISP: | Pružalac internet usluga |
| UPP: | Uzajamna pravna pomoć |
| NVO: | Nevladina organizacija |
| OSINT: | Obaveštajni podaci iz otvorenih izvora |
| THB: | Trgovina ljudima |
| TOR: | Onion Ruter |
| VOIP: | Protokol za prenos glasa putem interneta |

# Uvod

Internet, i uopšteno informaciono-komunikacione tehnologije (IKT), igraju važnu ulogu u oblikovanju naših života. Pandemija kovida-19 je jasno pokazala u kojoj meri su internet i IKT postali neizostavan deo različitih aktivnosti i društvenih interakcija - i ubrzala je njihov značaj. Svet kriminala nije izuzetak u tome – a to uključuje i trgovinu ljudima.

Nema sumnje da tehnologija donosi izazove – kao i mogućnosti – i za organe za sprovođenje zakona i za NVO. Istovremeno, baza dokaza o trgovini ljudima posredstvom interneta i tehnologije i dalje je ograničena i nepovezana. U ovom trenutku, najbolji dostupni dokazi potiču iz relativno malog broja studija, koje se obično zasnivaju na malom broju ispitanika među policijskim službenicima i predstavnicima NVO – najčešće sprovedenim u veoma ograničenom broju država – kao i na malobrojnim izveštajima međunarodnih organizacija. Ova studija prevazilazi granice anegdotalnih dokaza time što nudi analizu trgovine ljudima posredstvom interneta i tehnologije na osnovu dokaza koji su sistematski prikupljani od država ugovornica – potpisnica Konvencije Saveta Evrope (SE) o borbi protiv trgovine ljudima. Takvi dokazi su dopunjeni informacijama prikupljenim od NVO koje pružaju pomoć žrtvama trgovine ljudima, kao i od tehnoloških kompanija.

Oblast primene ove studije je relativno široka. Ona nudi procenu razmere u kojoj tehnologija utiče na trgovinu ljudima, kao i istraživanje modus operandija trgovaca ljudima u kontekstu trgovine ljudima posredstvom interneta i tehnologije. U osnovi ove studije leži istraživanje operativnih i pravnih izazova sa kojima se suočavaju države ugovornice – i u određenoj meri NVO – prilikom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom interneta i IKT, kao i prilikom identifikacije žrtava i podizanja nivoa svesti među ugroženim grupama. Ono što je ključno je da studija takođe istražuje strategije, alate i „dobre prakse" koje su usvojile države ugovornice i NVO u cilju prevazilaženja takvih izazova i unapređenja odgovora na trgovinu ljudima posredstvom interneta i tehnologije. Ovaj dokument otkriva sličnosti između država, kao i iskustva specifična za određene države. Poseban akcenat je stavljen na obuke – kao ulaganja u ljudski kapital, one su jednako važne kao ulaganja u tehničke alate.

Ova studija je sprovedena kao deo višegodišnjeg interesovanja Saveta Evrope za pitanje tehnologije i trgovine ljudima. Pored toga što nudi sistematsku procenu trenutno dostupne baze dokaza, ova studija takođe ima za cilj da pruži Grupi eksperata Saveta Evrope za borbu protiv trgovine ljudima (GRETA) i drugim subjektima alat za sprovođenje budućih procena i praćenje promena u oblasti tehnologije i ponašanja.

## *Metodologija*

Dokazi izneti u ovoj studiji prikupljeni su pomoću novog upitnika koji je sadržao pitanja otvorenog i zatvorenog tipa. Upitnik je pripremljen u tri verzije (priložene u Prilozima): duža verzija za države ugovornice (40 pitanja) i dve kraće verzije za NVO (14 pitanja) i tehnološke kompanije (11 pitanja). Dizajn upitnika zasniva se na analizi okruženja koja je sprovedena između oktobra i decembra 2020. godine i obuhvata različite izvore: međunarodne organizacije, akademsku zajednicu, NVO, kao i privatan sektor (videti Aneks A za više detalja). Upitnik je pripremljen u saradnji sa članovima GRETA i Sekretarijatom Saveta Evrope u periodu od januara do marta 2021. godine. Prikupljeni su odgovori od 40 država ugovornica[1], 12 NVO[2] i 2 tehnološke kompanije[3] tokom juna i jula 2021. godine (jedan zakasneli odgovor stigao je do Sekretarijata Saveta Evrope u septembru 2021. godine). Analize su rađene u periodu između juna i septembra 2021. godine. To je relativno kratak rok za studiju koja je obuhvatala prilično širok spektar problema, država i subjekata. Iako ova studija pruža detaljnu procenu velike količine dokaza, ona ni u kom slučaju nije sveobuhvatna niti bez ograničenja. O tome će biti više reči u nastavku teksta, kada to bude relevantno.

Ova studija primenjuje definiciju Latonera (2012: 9–10) da tehnologija predstavlja „informacione i komunikacione tehnologije, naročito one koje čine digitalna i umrežena okruženja. Tehnologije koje omogućavaju korisnicima da razmenjuju digitalne informacije putem mreža uključuju internet, onlajn društvene mreže i mobilne telefone."

Tehnologija će opstati – a sa njom i strukturne promene u načinu rada počinilaca krivičnih dela, otvaranje mogućnosti i pogoršanje postojećih ranjivosti. Stoga postoji potreba da države ugovornice usvoje i opreme svoje agencije za sprovođenje zakona i sisteme krivičnog pravosuđa mogućnostima za praćenje ovog okruženja koje se (neprekidno) menja. Ova studija u tom smislu pruža preporuke zasnovane na dokazima.

1 Albanija; Jermenija; Austrija; Azerbejdžan; Bosna i Hercegovina; Belorusija; Belgija; Bugarska; Hrvatska; Kipar; Danska; Estonija; Finska; Francuska; Nemačka; Grčka; Mađarska; Island; Irska; Letonija; Litvanija; Luksemburg; Malta; Republika Moldavija; Monako; Crna Gora; Holandija; Severna Makedonija; Norveška; Poljska; Portugal; Rumunija; San Marino; Slovačka; Slovenija; Španija; Švedska; Švajcarska; Ukrajina i Ujedinjeno Kraljevstvo.

2 Astra (Srbija); Different and Equal (Albanija); FIZ (Švajcarska); Hope Now (Danska); Jesuit Refugee Service (Severna Makedonija); KOK (Nemačka); La Strada (Republika Moldavija); La Strada International (širom Evrope); Migrant Rights Centre (Irska); Praksis (Grčka); Schweizer Plattform gegen Menschenhandel (Švajcarska); Sustainable Rescue Foundation (Holandija).

3 Facebook i IBM.

# Rezime izveštaja

## Uticaj tehnologije na trgovinu ljudima

Uticaj tehnologije na trgovinu ljudima naročito je važan u dve faze procesa trgovine: tokom **regrutovanja** i **eksploatacije**. Dokazi koje su dostavile države ugovornice ukazuju na sve „veći" značaj tehnologije u kontekstu trgovine ljudima, pri čemu većina država ugovornica sada smatra da je uticaj tehnologije na trgovinu ljudima „veoma važan" ili „važan".

Države ugovornice ukazuju na sve veći značaj onlajn materijala, reklama/oglasa i stranica/aplikacija za traženje posla, kao i na sve veći značaj onlajn socijalizacije i ličnih interakcija. Sa druge strane, oba ova segmenta stvaraju prilike za počinioce u oblasti trgovine ljudima i pogoršavaju postojeće ranjivosti. Tehnologija je promenila način interakcije među ljudima što se odražava i na svet kriminala, uključujući i trgovinu ljudima. Ovo je strukturna promena kojoj organi za sprovođenje zakona i sistemi krivičnog pravosuđa moraju da se prilagode.

Tehnologija može da igra ulogu u fazi **regrutovanja** time što olakšava identifikaciju, lociranje i uspostavljanje kontakta sa potencijalnim žrtvama. U zavisnosti od tipa eksploatacije, koriste se različiti mehanizmi.

U kontekstu regrutovanja u svrhu **seksualne eksploatacije**, nekoliko država ugovornica je otkrilo slučajeve oglasa za posao koji su bili povezani sa trgovinom ljudima i dokaze regrutovanja preko platformi društvenih medija, kao i aplikacija za upoznavanje. Uobičajena strategija je takozvana **tehnika „ljubavnika"**: vrsta regrutovanja putem interneta gde trgovac ljudima identifikuje i stupa u kontakt sa potencijalnom žrtvom preko onlajn platforme, upoznaje njene hobije i interesovanja, kao i ličnu i porodičnu situaciju. Trgovac ljudima potom pruža empatiju i podršku potencijalnoj žrtvi u kontekstu romantičnog odnosa – želi da uspostavi poverenje, a time i kontrolu nad žrtvom.

Dostupno je obilje dokaza iz više zemalja o slučajevima **ucene** žrtava. Ovo se najčešće postiže time što se prvo prikupe „kompromitujuće" informacije o žrtvama – na primer, time što se traže fotografije ili video-snimci nagog tela – i potom koriste te informacije da se osoba prisili na prostituciju.

Tokom **faze eksploatacije**, tehnologija može da omogući **prodaju** seksualnih usluga koje pružaju žrtve trgovine ljudima. Dostupno je obilje dokaza iz više zemalja o internet stranicama koje se koriste za reklamiranje seksualnih usluga. Među takvim reklamama nalaze se i usluge koje pružaju žrtve trgovine ljudima. Štaviše, dok se emitovanje uživo najčešće povezuje sa seksualnim zlostavljanjem dece, više država je ukazalo na činjenicu da emitovanje uživo može takođe da uključuje i odrasle žrtve trgovine ljudima.

Osim toga, tehnologija može da se koristi za **koordinaciju aktivnosti**. Ono što je ključno je da tehnologija omogućava **razdvajanje** između mesta gde se seksualna aktivnost izvodi i mesta gde se vrši koordinacija. Ovo ima važne implikacije u pogledu sprovođenja zakona.

Države su pružile dokaze o tehnološkim alatima koje trgovci ljudima koriste za **praćenje i kontrolu** žrtava tokom faze eksploatacije. Ucene i kompromitujuće informacije se takođe koriste protiv žrtava kao sredstvo kontrole tokom ove faze.

Brojne države prijavljuju pojavu trendova u kontekstu seksualne eksploatacije koji uključuju sve češću upotrebu „veb kamera za prenos uživo" i aplikacija za video-ćaskanje „plati koliko koristiš", kao i sve veću upotrebu aplikacija za kontrolu žrtava. Takve veb kamere i aplikacije za video-ćaskanje mogu se koristiti za emitovanje seksualnih radnji koje izvode žrtve trgovine ljudima uživo. Nekoliko država je navelo da je pandemija kovida-19 povećala mogućnosti za trgovce ljudima za uspostavljanje kontakta putem interneta sa ranjivim pojedincima.

U kontekstu trgovine ljudima u svrhu **radne eksploatacije**, dokazi koje su pružile države ugovornice ukazuju da se IKT prvenstveno koriste za **regrutovanje** žrtava, naročito posredstvom **oglasa za posao na internetu**. Takvi oglasi se ne objavljuju samo na stranicama rezervisanim za traženje posla, već i na društvenim medijima u specijalizovanim grupama za traženje posla i u grupama za uzajamnu pomoć. Nekoliko država je naglasilo značaj veb stranica koje imaju za cilj omogućavanje razmene informacija među radnicima migrantima koje trgovci ljudima koriste kao prostor za regrutovanje.

Trend u nastajanju u kontekstu radne eksploatacije, koji su prijavile neke države, uključuje povećanje broja slučajeva regrutovanja putem interneta i društvenih mreža. Veruje se da je ovom trendu doprinela pandemija kovida-19. Iako se čini da tehnologija ne igra značajnu ulogu u fazi eksploatacije, države su prijavile povećanje mogućnosti za eksploataciju žrtava trgovine ljudima koje donosi ekonomija honorarnih poslova („gig ekonomija"), naročito platforme za isporuku.

Nema dokaza relevantne uloge koju **mračna mreža** igra u kontekstu trgovine odraslim ljudima (cirkulacija materijala za seksualnu eksploataciju dece nije obuhvaćena oblašću primene ove studije). Slično tome, čini se da korišćenje **kriptovaluta** nije rasprostranjeno u kontekstu trgovine ljudima (sa druge strane, kriptovalute se koriste za kupovinu pristupa prenosu seksualnog zlostavljanja dece uživo).

Dokazi koje su pružile **NVO** prikazuju sličnu situaciju. One su primetile korišćenje interneta i društvenih medija tokom svih faza trgovine ljudima, naročito u vezi sa (a) regrutovanjem; (b) eksploatacijom; i (c) vršenjem kontrole i pritiska nad žrtvama. Pored toga, trgovci ljudima

koriste IKT, uključujući društvene medije i šifrovane aplikacije, kako bi nastavili da održavaju kontakt sa žrtvama trgovine ljudima nakon što napuste situaciju u kojoj se vrši eksploatacija, često kako bi ih sprečili da podnesu prijave i zatraže pravdu.

Novi trendovi primećeni u dokazima koje su pružile NVO ukazuju na povećanje eksploatacije dece putem **veb kamera i društvenih medija**. Navodi se i da su počinioci počeli da koriste **onlajn igrice** za stupanje u kontakt sa potencijalnim žrtvama.

Na kraju, dostupni dokazi ukazuju da upotreba tehnologije dopunjava, a ne zamenjuje lične interakcije van mreže. Tehnologiju i interakcije licem u lice je najbolje posmatrati kao integrisane.


# Izazovi tokom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom tehnologije

## Izazovi tokom otkrivanja

Otkrivanje slučajeva trgovine ljudima posredstvom interneta i tehnologije i identifikacija žrtava i dalje predstavljaju velike izazove. Države ugovornice ukazuju na brojne izazove:

- Neprekidno rastući broj onlajn aktivnosti/interakcija. Nadziranje interneta zahteva ogromne resurse i podleže pravnim ograničenjima (uključujući primenu zakona o privatnosti i ograničenja korišćenja sistema za skeniranje mreže radi prikupljanja podataka u nekim državama);
- Broj onlajn oglasa (otvorenih i malih oglasa) za seksualne i neseksualne usluge je često prevelik za ručno pretraživanje;
- Poteškoće prilikom identifikacije počinilaca i žrtava, jer mogu da koriste nadimke i pseudonime tokom svojih onlajn aktivnosti i mogu da koriste softver za anonimizaciju (npr. VPN);
- Korišćenje šifrovane komunikacije između trgovaca i žrtava. Konverzacija između trgovaca ljudima i žrtava odvija se u zatvorenim grupama;
- Ponašanje korisnika interneta koje se brzo menja;
- Izazovi prilikom sortiranja onlajn oglasa kako bi se identifikovali oni koji se odnose na trgovinu ljudima u kontekstu seksualnih i neseksualnih usluga. Znaci upozorenja na oglase povezane sa seksualnom i radnom eksploatacijom su i dalje nedovoljno razvijeni i nedovoljno se koriste;
- Nepostojanje specijalizovanih jedinica pri policiji i/ili odsustvo specijalizovanih istražitelja za slučajeve trgovine ljudima sa naprednim veštinama korišćenja računara. Nedostatak službenika koji su obučeni za izvođenje tajnih operacija na internetu. Sajber operacije mogu dugo da traju i da oduzimaju puno vremena;
- Proces slanja zahteva kompanijama koje upravljaju društvenim medijima koji oduzima mnogo vremena i odsustvo reakcije nekih od takvih kompanija;
- Kratki periodi čuvanja IP adresa i poteškoće oko pristupanja takvim podacima.

## Izazovi tokom istraga

Šifrovanje podataka predstavlja najozbiljniji izazov sa kojim se suočavaju države ugovornice (nivo ozbiljnosti 80 od 100). Nakon toga slede velika količina podataka (71), brzina tehnoloških promena (66), nedovoljna tehnička oprema (63), neodgovarajući zakonodavni alati (61), odsustvo tehničkih znanja među organima za sprovođenje zakona (53) i odsustvo pomoći privatnog sektora (46).

**Protokoli za šifrovanje podataka** koji se nalaze u popularnim aplikacijama i onlajn servisima smatraju se problematičnim. Šifrovanje takođe ograničava mogućnost praćenja komunikacije. Nekoliko država je nagovestilo postojanje alata za dešifrovanje nekih vrsta uređaja. Međutim, ovo je okruženje koje se neprekidno razvija i zahteva (velika) ulaganja u obuke i softver. Koraci preduzeti za prevazilaženje ovog problema uključuju uspostavljanje jedinica/centara za borbu protiv sajber-kriminala čiji zadatak je rad sa tehnologijom za dešifrovanje. Osim toga, veoma je značajno udruživanje resursa na nadnacionalnom nivou za potrebe razvoja tehnoloških proizvoda, kao što su softveri za dešifrovanje i skeniranje mreže radi prikupljanja podataka.

Elektronske komunikacije i IKT uređaji generišu **velike količine podataka koje neprekidno rastu**, a koje predstavljaju ogroman napor za istražitelje. Ovaj napor utiče na sposobnost istražitelja da izdvoje i pažljivo analiziraju podatke, što samo po sebi zahteva specijalizovani softver, kao i posebne obuke o sistematizaciji i pretraživanju tako velikih količina dokaza.

Postoji opšta saglasnost da je razvoj kapaciteta za rukovanje velikim količinama **elektronskih dokaza** od ključnog značaja. Međutim, takvi kapaciteti se moraju neprekidno modernizovati. Države su navele da izazovi sa kojima se suočavaju ne leže samo u sve većoj količini podataka koje generišu onlajn platforme i društveni mediji, već i u promenjivim **obrascima ponašanja** njihovih korisnika.

**Nedostatak tehničke opreme** prepoznat je kao izazov u nekoliko država. Specijalizovani softver i hardver je često veoma skup i zahteva konstantna ažuriranja i skupe ugovore o licenciranju kako bi se pratio korak sa brzinom tehnoloških promena. **Potreba da se prati korak sa tehnološkim promenama** može da ima značajan uticaj na budžet policije. Ovaj problem je prijavilo nekoliko država, bez obzira na njihov nivo BDP-a (bruto domaćeg proizvoda).

Ulaganja u ljudski kapital su jednako važna kao i ulaganja u softver i hardver, ako ne i važnija, posebno kada se odnose na **odsustvo razvoja i potrebu za razvojem tehničkih znanja među organima za sprovođenje zakona**. Dokazi ukazuju na potrebu za razvojem znanja o (a) pojavi novih trendova i promenama u upotrebi tehnologije; (b) pojavi novih aplikacija i usluga na tehnološkom tržištu koje karakterišu brze promene, i (c) razvoju novih bezbednosnih protokola i metoda šifrovanja. Ono što je najvažnije, znanje treba mudro rasporediti unutar organizacije. Na primer, nedostatak specijalizovanih službenika na lokalnom nivou može da stvori **uska grla u istragama**, ako je potrebno više puta tražiti pomoć od (preopterećene) centralizovane jedinice.

Nekoliko zemalja je istaklo potrebu za **organizovanjem dodatne tehničke obuke za sve policijske službenike**, uključujući za sticanje znanja o tehnologiji i kako ona funkcioniše. Slično tome, odgovarajuća obuka o pribavljanju i rukovanju **elektronskim dokazima** treba da bude obezbeđena za najveći broj relevantnih službenika i treba da bude redovna tema u nastavnim planovima i programima obuka za policijske službenike. U složenijim slučajevima

može biti potrebno formirati timove sa multidisciplinarnim veštinama (npr. okupiti istražitelje, finansijske stručnjake i stručnjake za sajber kriminal).

Dalji izazovi uključuju pitanja koja proizilaze iz neodgovarajućih **obaveza čuvanja podataka** nametnutih pružaocima internet usluga (ISP) i iz primene zakona o privatnosti, na primer u vezi sa sistemima za skeniranje mreže radi prikupljanja podataka.

## Izazovi tokom krivičnog gonjenja

Sve u svemu, izazovi sa kojima se sreće tužilaštvo imaju nižu ocenu od izazova tokom istraga, pri čemu je samo za „pribavljanje dokaza iz drugih zemalja" ocena nešto viša od 50 (od 100). Ovo je praćeno nedostatkom obuke među tužiocima (40); neodgovarajućim zakonodavnim alatima (38) i nedostatkom pomoći privatnog sektora (33). Čini se da ekstradicija osumnjičenih (28) i određivanje nadležnosti (16) igraju marginalnu ulogu.

Adekvatna **obuka tužilaca** smatra se ključnom za obezbeđivanje da predmeti koji se razvijaju uz pomoć IKT-a budu robusni, da se elektronski dokazi pravilno prikupljaju i koriste, i da se predmeti na odgovarajući način iznose pred sudijom/porotom. Neke države ugovornice primetile su slučajeve u kojima tužioci nisu bili upoznati sa procedurama za traženje elektronskih podataka od privatnih kompanija ili sa procedurama za pribavljanje dokaza i saradnje iz drugih zemalja (npr. putem zajedničkog istražnog tima – ZIT ili evropskog naloga za istragu – EIO).

Neke države ugovornice pokrenule su pitanje postupanja sa elektronskim materijalom, naročito u kontekstu **obaveza po osnovu GDPR** (Opšte uredbe EU o zaštiti podataka o ličnosti). Takođe je izražena zabrinutost oko međunarodnih propisa o zaštiti podataka koji mogu da ometaju prikupljanje, čuvanje i obradu informacija dobijenih primenom tehnoloških istražnih tehnika (kao što je skeniranje mreže radi prikupljanja podataka (*web crawling*)).

Primećeni su izazovi koji se tiču IP adresa i elektronskih dokaza. IP adrese treba da budu povezane sa korisničkim imenima i korisnicima kadgod je to moguće. Međutim, korisnička imena se mogu promeniti u bilo kom trenutku i osumnjičeni ih često koriste naizmenično.

Još jedan izazov odnosi se na **iznošenje dokaza** pred porotom (i sudijom), jer tehnički dokazi u slučajevima koji se razvijaju uz pomoć IKT-a mogu biti složeni i često je potreban stručnjak da ih izvede. Razvijanje interne stručnosti među službenicima o tome kako efikasno i tačno izvesti elektronske dokaze sve više dobija na značaju.

## Izazovi međunarodne saradnje

Velika većina država ugovornica naznačila je dugo vreme potrebno za obradu **zahteva za uzajamnu pravnu pomoć** (UPP) kao jednu od glavnih prepreka međunarodnoj saradnji. Procedure uzajamne pravne pomoći smatraju se sporim, ponekad nepredvidivim, a potrebni su im i međunarodno dogovoreni šabloni. Ovo pitanje je naročito otežano kada se saradnja odvija izvan pravnog okvira EU.

**Saradnja van pravnog okvira EU** posmatra se kao proces koji oduzima puno vremena i koji karakteriše veća zamršenost zbog nedostatka usaglašenosti između različitih pravnih si-

stema, uz elemente nepredvidivosti i nedoslednosti. Jasnije operativne procedure, poboljšana redovna razmena između kontaktnih tačaka, jasno utvrđivanje zahteva za međunarodnu pravnu pomoć i diskusija na samom početku doprineli bi usaglašavanju procesa.

Tehnologija omogućava kriminalnim mrežama da organizuju i kontrolišu aktivnosti eksploatacije na daljinu – na primer, iz druge zemlje – često znajući da zahtevi za pravosudnu saradnju neće biti blagovremeno realizovani, ako uopšte budu. Ovo stvara potrebu za unapređenjem ili u nekim slučajevima uspostavljanjem sporazuma sa državama porekla žrtava ako se nalaze izvan EU.

Izazovi u obradi zahteva za UPP takođe mogu biti rezultat **nedostatka adekvatno obučenog osoblja** za formulisanje i upravljanje zahtevima, kao i korišćenja zastarele tehnologije.

Elektronski dokazi mogu otežati identifikaciju tačne lokacije podataka i države u čijoj nadležnosti se ti podaci nalaze, što otežava formulisanje zahteva za uzajamnu pravnu pomoć.

Upućeni su pozivi za uspostavljanje zajedničkog pravnog okvira za **brzu razmenu digitalnih dokaza**. Nekoliko država je izrazilo zabrinutost zbog nepostojanja homogene regulative o **čuvanju podataka**, što ometa razmenu elektronskih dokaza. Sve u svemu, države ugovornice su izrazile potrebu za sveobuhvatnijim okvirom koji uređuje čuvanje i prenos elektronskih dokaza i za zajedničkim pravnim okvirom koji bi zamenio trenutne *ad hoc* bilateralne radne sporazume između država i privatnih kompanija koje drže podatke (videti u nastavku). Države ugovornice su takođe istakle potrebu da se unapredi razmena podataka tokom istraga.

## Izazovi tokom saradnje sa privatnim kompanijama

Nekoliko država je navelo da su ISP (pružaoci internet usluga), pružaoci sadržaja i kompanije koje nude društvene medije generalno sarađivali u pogledu pitanja vezanih za trgovinu ljudima i seksualnu eksploataciju dece. Ipak, identifikovani su brojni izazovi. Oni uključuju:

- **Dobijanje blagovremenog odgovora** od nekih ISP i pružalaca sadržaja. Obraćanje hostovima putem zamolnica poslatih preko relevantnih institucija može dovesti do dugog čekanja sa rizikom da sadržaj bude izbrisan do trenutka kada se postupi po zahtevu;
- **Pojašnjavanje pravnih zahteva** u skladu sa kojima IKT kompanije i pružaoci internet usluga funkcionišu. Neke države su izrazile zabrinutost da neki ISP nameću formalističke i „pravno neopravdane" zahteve agencijama za sprovođenje zakona i ne obrazlažu i ne objašnjavaju odbijanja na odgovarajući način;
- **Nedostatak određene kontakt tačke** u privatnim kompanijama. Velike kompanije koje posluju u više država često nemaju osoblje koje poseduje jezičke i pravne veštine relevantne za svaku državu u kojoj posluju;
- **Nedostatak znanja** među pružaocima sadržaja i kompanijama koje pružaju društvene medije o tome koja je nacionalna agencija odgovorna za koje odluke, npr. uklanjanje nezakonitog sadržaja. Bilo je predloga da se uvede uloga „pouzdanog čuvara sadržaja", odnosno da se odrede određene agencije koje bi imale zadatak da se povežu sa međunarodnim pružaocima usluga radi uklanjanja sadržaja. Pouzdani čuvar sadržaja bi imao otvoren kanal komunikacije sa kompanijama i izgradio bi uzajamno poverenje.

## Dokazi prikupljeni od NVO

Uopšteno govoreći, dokazi prikupljeni od NVO ukazuju na slične probleme koji su razmotreni iznad. Konkretnije, NVO su istakle sledeće probleme:

- **Nedostatak kapaciteta** organa za sprovođenje zakona, što uključuje nedostatak obuke, hardvera i softvera i ograničenu upotrebu posebnih istražnih tehnika. Takođe postoji nedostatak specijalizacije među nekim policijskim snagama i pravosuđem u vezi sa trgovinom ljudima posredstvom tehnologije;
- **Tehnološko okruženje koje se brzo menja i *modus operandi* počinilaca**. Profesionalcima je teško da prate korak sa trgovinom ljudima posredstvom tehnologije, što ometa njihovu sposobnost da brzo identifikuju slučajeve. Znanje o tehničkom okruženju i praksama (*modus operandi*) se često ne razmenjuje;
- Korišćenje privatnih foruma, soba za ćaskanje ili šifrovanih aplikacija za kontakte između počinilaca i žrtava. Ovo otežava (a) otkrivanje takvih kontakata i (b) njihovo pribavljanje kao dokaza koji će se koristiti na sudu. NVO su predložile navođenje informacija/upozorenja o bezbednom korišćenju privatnih kanala komunikacije u sobama za ćaskanje i aplikacijama;
- **Pravila o zaštiti podataka i privatnosti** mogu da ometaju identifikaciju žrtava, kao i trgovaca ljudima. Pravila propisana GDPR-om ograničavaju upotrebu tehnologije za otkrivanje digitalnih tragova koje ostavljaju i žrtve i počinioci;
- **Nedostatak interdisciplinarne tehnološke saradnje** između privatnih kompanija, javnih agencija i NVO kako bi se u potpunosti iskoristila sve veća količina podataka o trgovini ljudima;
- **Nedostatak tehnološke strategije** u nacionalnim akcionim planovima za borbu protiv trgovine ljudima;
- **Nedostatak kapaciteta, resursa i tehničkih alata** NVO za redovno otkrivanje onlajn eksploatacije posredstvom tehnologije;
- **Suprotstavljeni ciljevi** ili različiti pristupi NVO i organa za sprovođenje zakona.

## Dokazi prikupljeni od tehnoloških kompanija

Kao što je navedeno iznad, samo dve kompanije su dostavile odgovore na upitnik. Kompanija Facebook je primetila da korisnici „retko prijavljuju" sadržaje koji se odnose na trgovinu ljudima. Kompanija IBM je primetila nekoliko prepreka za saradnju sa organima za sprovođenje zakona, uključujući zabrinutost u vezi sa zakonitošću takve saradnje, posebno u vezi sa privatnošću podataka i pravnom složenošću situacije koja uključuje nadležnost više država. IBM je takođe zatražio pojašnjenja o međunarodnim pravnim dozvolama za prikupljanje i deljenje podataka sa organima za sprovođenje zakona.

## Strategije i dobre prakse

### Otkrivanje slučajeva trgovine ljudima posredstvom IKT

Države su navele da primenjuju različite strategije za otkrivanje slučajeva trgovine ljudima posredstvom interneta i IKT. Često se navodi strategija **nadgledanja interneta**, uključujući foruma i, u nekim slučajevima, TOR mreže (mračne mreže). Ovo je kombinovano sa upotrebom **obaveštajnih podataka iz otvorenih izvora (OSINT)**, što znači prikupljanje podataka sa društvenih medija i iz drugih javno dostupnih onlajn izvora o mreži kontakata određenog lica, njegovim životnim uslovima i finansijskoj situaciji.

Neke države su formirale **„sajber patrole" sa specijalizovanim službenicima** zaduženim za sprovođenje OSINT istraga na internetu. Neke države dozvoljavaju tajne istrage na internetu (sajber infiltracija).

Neke agencije za sprovođenje zakona koriste **alate za „struganje" interneta** posebno razvijene za izdvajanje informacija sa veb lokacija, naročito za identifikaciju rizika i ranjivosti na veb lokacijama za usluge za odrasle (ASW).

Vezano za OSINT istrage, koriste se **tehnike analize društvenih mreža** kako bi se razumele i rekonstruisale mreže kontakata počinioca i/ili žrtve. **Relacione informacije** su ključne: informacije prikupljene iz različitih izvora mogu se sistematizovati i koristiti **za rekonstrukciju kriminalnih mreža**, odnosno odnosa između mesta, počinilaca i žrtava.

Međutim, nisu sve države ugovornice navele da koriste „proaktivne" strategije. Nekoliko država ugovornica je navelo da njihove istrage o trgovini ljudima posredstvom IKT ostaju „reaktivne".

Nekoliko država je implementiralo **sisteme pomoću kojih korisnici interneta mogu da prijave sadržaje i veb lokacije** za koje sumnjaju da su povezani sa nezakonitim aktivnostima, uključujući seksualnu i radnu eksploataciju. U nekim državama, na primer, u Francuskoj,

pružaoci internet usluga i veb lokacija su dužni da pomognu organima za sprovođenje zakona u borbi protiv širenja materijala koji se odnose na određena krivična dela, uključujući trgovinu ljudima. Od njih se zahteva da uspostave lako dostupan i vidljiv sistem koji omogućava svakom pojedincu da označi sumnjivi materijal.

Neke države su prijavile organizovanje **kampanja za podizanje svesti** za povećanje otkrivanja slučajeva trgovine ljudima posredstvom IKT. To uključuje kampanje za podizanje svesti usmerene ka klijentima koji koriste veb lokacije na kojima se nalaze oglasi za seksualne usluge kako bi ih informisali o riziku od slučajeva trgovine ljudima (Belgija i Ujedinjeno Kraljevstvo) i kampanje koje pružaju informacije o tome kako pronaći bezbedne prilike za zapošljavanje (Poljska i Bugarska). Nadležni organi nekih država koristili su društvene medije za širenje ciljanih informacija, ponekad uz kreiranje ciljanih Facebook reklama povezanih sa linijom za dojavu.

## Istraga slučajeva trgovine ljudima posredstvom IKT

U nekim državama, agencije za sprovođenje zakona sprovode **sajber infiltraciju** u kriminalne mreže koristeći prikrivene tehnike, kao i tajne istrage. Nekoliko država je izrazilo potrebu za povećanjem broja takvih **tajnih istraga**, zbog čega ulažu u obuku specijalizovanih službenika. Postoji opšta saglasnost o značaju nabavke i pristupanju **specijalizovanom softveru**, kao i o značaju velikih količina podataka i poboljšanja mogućnosti u pogledu velikih količina podataka. Takođe je ključan razvoj alata za preuzimanje informacija sa mobilnih telefona bez otkrivanja šifre i za dešifrovanje razgovora preko aplikacija za komunikaciju.

Smatra se da je **ulaganje u ljudski kapital** jednako ključno kao i ulaganje u tehnološku opremu. Ulaganje u ljudski kapital može da podrazumeva da se službenicima za sprovođenje zakona obezbede kontinuirane obuke i aktivnosti razvoja zasnovane na najboljim lokalnim i globalnim praksama. Isto tako, nekoliko država je ukazalo na značaj uključivanja specijalizovanih istražnih službenika sa „digitalnim znanjem" u istrage slučajeva trgovine ljudima. Jedan model bi podrazumevao prisustvo osoblja posebno obučenog za sprovođenje istraga na internetu i društvenim mrežama koje je integrisano u svaku jedinicu specijalizovanu za borbu protiv trgovine ljudima. Time bi se formirale **grupe za tehničku podršku** istražiteljima. U takvim grupama mogu biti policijski službenici sa policijskim ovlašćenjima ili ostali policijski službenici. Ova ideja se **udaljava od tradicionalnog policijskog modela** zasnovanog na policajcima pod zakletvom i usvaja principe – koje već primenjuju neke policijske uprave – da službenici koji nisu pod zakletvom imaju više tehničku ulogu (npr. analitičari).

Osim toga, države ugovornice su istakle značaj **međuagencijskog istražnog rada** uz učešće i saradnju širokog spektra specijalizovanih agencija – kao i značaj razmene znanja među institucijama. Slično tome, države su ukazale na značaj **unapređenja prekogranične saradnje** kroz, na primer, međusobnu razmenu službenika sa državama porekla žrtava. Na operativnom nivou, države su napomenule da bi istraga mogla biti olakšana **lakšim čuvanjem dokaza na međunarodnom nivou i pristupom takvim dokazima**.

Prilikom sprovođenja istraga, sugerisano je da države ne bi trebalo previše da se oslanjaju na **preskriptivnu listu indikatora**, npr. da identifikuju visokorizične reklame/oglase na internetu, već da se takođe oslanjaju na slojevitost informacija različite prirode, uključujući obaveštajne podatke, informacije iz otvorenih izvora i policijskih evidencija. Naglašen je **značaj analize mreže i relacionih podataka**.

Iako oduzima puno vremena, **strateška analiza** koja generiše znanje o novim trendovima i ažurirane informacije o *modus operandiju* počinilaca (uključujući tehnologiju i veb lokacije koje koriste počinioci) smatra se veoma značajnom.

Tehnologija se takođe može koristiti za **olakšavanje prikupljanja dokaza od žrtava** i tokom istrage i krivičnog gonjenja predmeta trgovine ljudima, kao i za smanjenje opterećenja za žrtve.

## Podsticanje međunarodne saradnje

Države ugovornice su prepoznale sledeće dobre principe za podsticanje međunarodne saradnje:

- Korišćenje resursa dostupnih u agencijama kao što su Evropol i Evrodžast, i uspostavljanje zajedničkih istražnih timova (ZIT) za one države koje su deo pravosudnog okvira EU;
- Uspostavljanje kontakata sa drugim zainteresovanim stranama u ranoj fazi istrage;
- Razvijanje veoma dobrog razumevanja pravnog konteksta i mogućnosti saradnje sa drugim državama;
- Organizovanje koordinacionih sastanaka radi razmene informacija i dokaza što je brže moguće i kako bi se utvrdila zajednička strategija od *samog početka*;
- Razvijanje zajedničkog razumevanja standardizovanih pristupa i obezbeđivanje transnacionalne interoperabilnosti agencija za sprovođenje zakona kroz transnacionalne obuke.

Saradnja među nepolicijskim organima, koja se često zanemaruje, može biti jednako relevantna kao i saradnja sa policijskim organima, naročito u kontekstu trgovine ljudima u svrhu radne eksploatacije (npr. između inspektorata rada).

## Identifikacija žrtava i pomoć

Čini se da se **prepoznavanje lica** često koristi u slučajevima seksualne eksploatacije dece (CSE). Međutim, čini se i da je upotreba ove tehnike ograničenija izvan konteksta seksualne eksploatacije dece. Nekoliko država je ukazalo na upotrebu tehnoloških alata za identifikaciju žrtava trgovine ljudima koji koriste velike količine podataka (uglavnom sistema za skeniranje mreže radi prikupljanja podataka, ali i alata za prepoznavanje lica pod strožim uslovima).

Nekoliko država se oslanja na indikatore za identifikaciju slučajeva trgovine ljudima („**znake upozorenja**"); međutim, ovo su „opšti" indikatori trgovine ljudima i nisu specifični za trgovinu ljudima posredstvom IKT-a. Iako postoji jasna potreba da se razviju indikatori specifični za trgovinu ljudima posredstvom IKT, nadležni organi su takođe upozorili da se ne treba previše oslanjati na „znake upozorenja". Čak i u slučajevima u kojima su indikatori konkretno razvijeni za identifikaciju žrtava na veb lokacijama za usluge za odrasle (ASW), kao što je slučaj u Ujedinjenom Kraljevstvu, indikatori pokazuju neka jasna ograničenja i najbolje ih je koristiti u kombinaciji sa **analizom društvenih mreža i ljudskom procenom** dokaza.

Tehnološki alati mogu biti veoma dragoceni u vršenju redukcije podataka i rukovanju velikim količinama informacija; međutim, potrebno je da ih koriste dobro obučeni operateri koji su upoznati sa specifičnom temom/problemom (npr. trgovina ljudima). Korišćenje veštačke inteli-

gencije i tehnoloških alata za identifikaciju žrtava nije bez problema, uključujući etička pitanja i mogućnost diskriminacije (npr. profilisanje zasnovano na diskriminatornim kriterijumima; videti u nastavku).

Što se tiče inicijativa zasnovanih na tehnologiji za pomoć žrtvama i širenje informacija ugroženim zajednicama, države su identifikovale primere (1) onlajn mehanizama za samoprijavljivanje i telefonskih linija za pomoć, uključujući digitalnu pomoć putem funkcije ćaskanja; (2) onlajn kampanja za podizanje svesti koje su često usmerene na određene rizične grupe (npr. osobe koje traže posao); (3) namenski razvijenih aplikacija i onlajn alata; i (4) zvaničnih materijala koji su dostupni onlajn i prevedeni na nekoliko jezika. Dobra praksa je rad sa privatnim kompanijama na izradi **društvenog oglašavanja** (na primer, zajednički razvoj sa društvenim medijima i sponzorisanje od strane društvenih medija). Međutim, onlajn kampanje ne bi trebalo da zamene direktne, lične kontakte sa ranjivim pojedincima.

## Dokazi prikupljeni od NVO

Nevladine organizacije su naglasile značaj postojanja **odgovarajućih i ažuriranih informacija** kojima žrtve trgovine ljudima i oni koji su podložni eksploataciji i zlostavljanju mogu lako da pristupe putem interneta. Takve onlajn platforme takođe treba da **omoguće samoidentifikaciju** žrtava. Ovo bi trebalo da se kombinuje sa **kampanjama za podizanje svesti**.

NVO su dalje istakle značaj razvoja znanja o rizicima vezanim za IKT i uopšteno o trgovini ljudima posredstvom tehnologije, takođe među organizacijama koje pomažu žrtvama, uključujući one koje pružaju savetodavne usluge. Pošto je **očuvanje elektronskih dokaza** ključno za razvoj jakih istraga, od izuzetnog je značaja da savetnici i NVO na prvoj liniji borbe budu upoznati sa strategijama za očuvanje digitalnih dokaza (npr. čuvanjem istorija ćaskanja).

Dokazi prikupljeni od NVO potvrđuju da „**znaci upozorenja**" u slučajevima trgovine ljudima posredstvom tehnologije nisu u širokoj upotrebi. NVO prijavljuju korišćenje standardnih indikatora, ali pozivaju na **reviziju takvih indikatora** kako bi se razmotrile specifičnosti IKT posredstvom tehnologije.

NVO su identifikovale primere **inicijativa zasnovanih na tehnologiji** koje su razvile da (a) podstiču samoprijavljivanje putem interneta; (b) uspostave kontakt sa rizičnom populacijom, na primer, da razbiju izolaciju i osnaže žrtve; (c) podižu svest među ranjivim i rizičnim grupama i omoguće traženje pomoći putem namenski napravljenih aplikacija i veb lokacija; i (d) sprovode kampanje za podizanje svesti putem interneta.

Uopšteno govoreći, NVO sve više koriste tehnologiju, ali njihov opšti nivo i dalje ostaje „ograničen". Postoji opšta saglasnost da se više može učiniti kako bi se bolje iskoristila tehnologija, naročito u pogledu načina na koji se tehnologija koristi za širenje informacija; za pristupanje potencijalnim žrtvama i komunikaciju sa njima; i za primanje dojava i prijava.

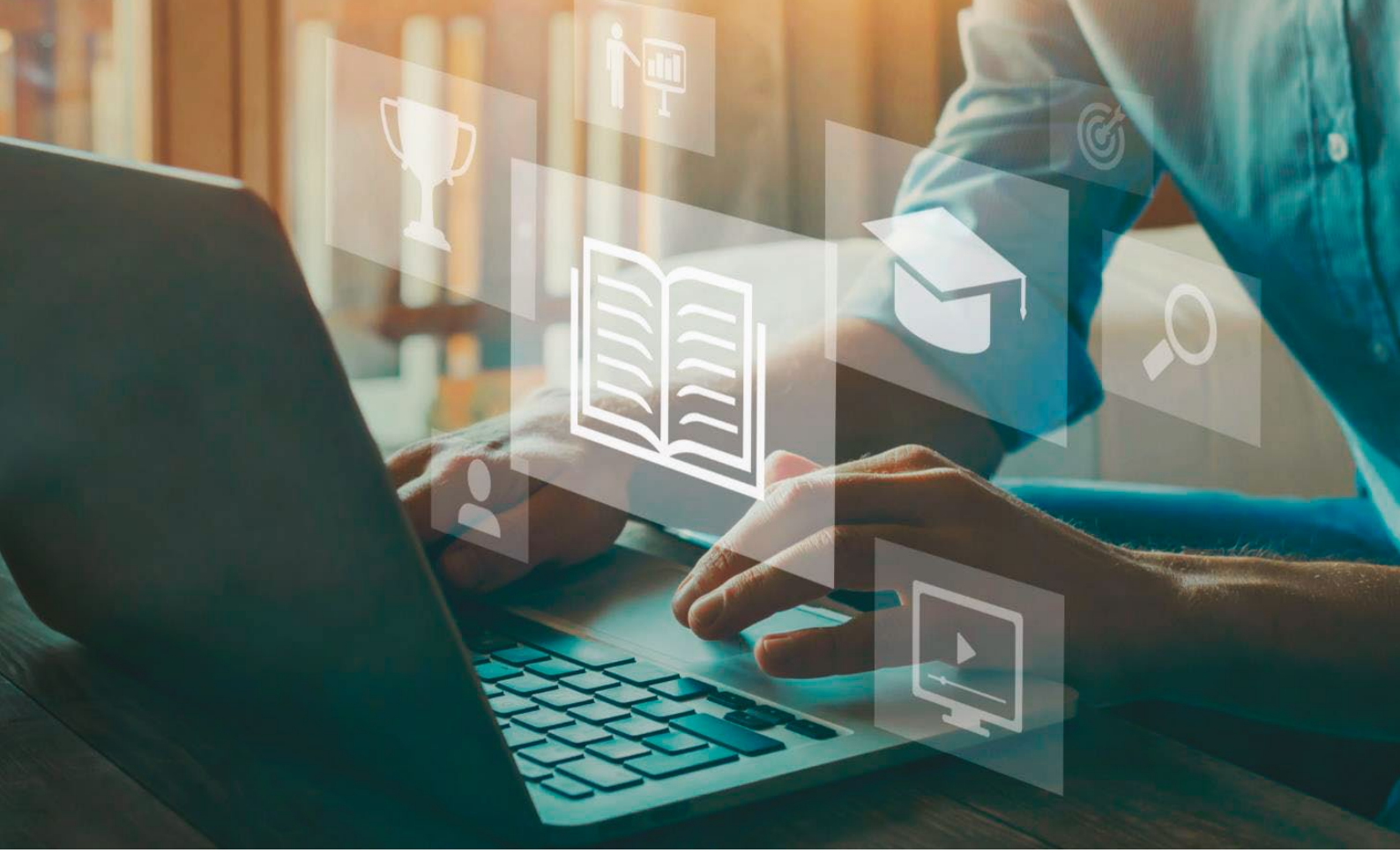
NVO su takođe otvorile neka **kritična pitanja** u vezi sa inicijativama i tehnološkim alatima, uključujući potrebu za periodima testiranja novih alata i – što je najvažnije – dokazima o njihovoj efikasnosti (koji su još uvek veoma ograničeni). One pozivaju na **više evaluacije i procene uticaja** razvijenih tehnoloških alata. Pored toga, često ne postoji dugoročna finansijska strategija za promovisanje i korišćenje razvijenih alata, uključujući resurse za njihovo ažuriranje. NVO su takođe naglasile da, uopšteno posmatrano, još uvek postoji ograničena

dostupnost tehnoloških **alata koje praktičari *mogu* da koriste** (da bi odgovarali potrebama NVO, alati moraju biti „jeftini i „jednostavni za upotrebu").

## Dodatni dokazi prikupljeni na osnovu analize okruženja

Ostala pitanja otvorena u dostupnoj bazi dokaza uključuju sledeća:

- Potrebu da se deluje na osnovu informacija koje se koriste kroz tehnologiju (u slučaju o kome su raspravljali Rende Taylor i Shih (2019), pokazalo se da se retko reaguje na izveštaje radnika podnete putem aplikacije za prijavu povratnih informacija o eksploataciji u lancima snabdevanja);
- Tehnologiju ne treba posmatrati kao zamenu za praktično znanje na terenu;
- Grupno delovanje za potrebe otkrivanja žrtava može da otvori pitanja privatnosti, kao i potencijalnog rizika od osvete. Dok se saveti korisnika smatraju veoma dragocenim, inicijative za grupno delovanje moraju biti pažljivo ispitane i uravnotežene u odnosu na rizik stvaranja virtuelnih (i nevirtuelnih) grupa osvetnika;
- Potreba da se unaprede prikupljanje i analiza digitalnih dokaza u cilju smanjenja opterećenja za žrtve (npr. kada se od njih traži da pruže dokaze protiv trgovaca ljudima ili u njihovu odbranu).



## Obuka: šta je obezbeđeno, šta je potrebno

Ogromna većina država je prijavila da organizuje obuke o trgovini ljudima. Međutim, nivoi i formati obuka koje se organizuju za **organe za sprovođenje zakona** razlikuju se od države do države. Neke države zahtevaju od svih policajaca koji bi mogli doći u kontakt sa potencijalnom žrtvom da prođu obuku, dok druge ograničavaju obuku na specijalizovane jedinice.

Postoji opšta saglasnost o činjenici da službenici treba da prođu obuku o (a) načinu otkrivanja slučajeva trgovine ljudima i žrtava; (b) načinu prikupljanja, čuvanja i obrade elektronskih dokaza, uključujući metode izdvajanja informacija iz računara i drugih digitalnih medija; i (c) načinu korišćenja relevantnog softvera, uključujući „**analizu velikih količina podataka**" i sistema za skeniranje mreže radi prikupljanja podataka (gde to dozvoljava nacionalno zakonodavstvo). Nekoliko država smatra da je neophodna **obuka o OSINT-u**. Istražne tehnike koje uključuju **tajne istrage na internetu** takođe se smatraju sve važnijim.

Iako je većina država prijavila obezbeđivanje elemenata gore pomenutih obuka, one su takođe naglasile probleme, uključujući (a) potrebu da se obuka održi aktuelnom i, u nekim slučajevima, da se značajno unaprede postojeći elementi; i (b) da se poveća procenat osoblja koje prolazi obuku. Neke države su izrazile zabrinutost zbog ograničenih obuka koje se često pružaju kada je reč o pitanjima povezanim sa IKT i, još više, trgovinom ljudima posredstvom IKT.

Gledajući u budućnost, **rizik od uskih grla u sistemu** je posebno akutan. S obzirom da će se zločini posredstvom IKT-a, uključujući trgovinu ljudima, verovatno neprekidno povećavati, postoji potreba da se ne oslanjamo previše na centralizovane centre za borbu protiv visokotehnološkog (sajber) kriminala. Ključno je uključiti opšte/osnovno **znanje o visokotehnološkom kriminalu** u rutinske obuke koje se organizuju za istražitelje, a ne da se na to gleda kao na skup „specijalizovanih" veština kako bi se izbegla takva uska grla.

**Šest širokih oblasti se smatra ključnim za izgradnju kapaciteta**: prikupljanje i analiza informacija iz otvorenih izvora (OSINT); prikupljanje podataka sa profila društvenih mreža i aplikacija za komunikaciju, kao i sa mračne/TOR mreže; ispitivanje informacija koje se nalaze na uređajima za komunikaciju i čuvanje informacija, uključujući informacije koje su korisnici izbrisali, kao i znanje o šifrovanju; sposobnost da se podaci dobijeni iz IKT izvora potkrepe dodatnim dokazima prikupljenim tokom krivične istrage; identifikacija žrtava/potencijalnih žrtava u onlajn okruženju; obuka o ekonomskom i finansijskom kriminalu sa elementom posvećenim onlajn transakcijama i potencijalno kriptovalutama.

Organizovanje **obuka za tužioce i sudije** u vezi sa trgovinom ljudima posredstvom IKT prilično je neujednačeno u različitim državama ugovornicama. Nekoliko država je navelo da trenutno ne organizuje nikakve obuke za pravosuđe o ovoj pojavi. Druge države organizuju opšte obuke o trgovini ljudima bez elemenata posebno fokusiranih na pitanja vezana za IKT.

**NVO** su izrazile potrebu da im domaći organi za sprovođenje zakona i međunarodne organizacije organizuju obuke o najnovijim dostignućima u tehnološkom okruženju i u oblasti trgovine ljudima, uključujući promene u strategijama regrutovanja. Takođe su istakli potrebu za obukama o najboljim međunarodnim praksama i razmeni iskustava među državama.

# Pravni instrumenti

## Nedostaci postojećeg međunarodnog okvira

Uopšteno posmatrano, države ugovornice su izrazile pozitivan stav o dostupnim pravnim instrumentima koji omogućavaju saradnju među državama u borbi protiv trgovine ljudima. Konvencije SE o uzajamnoj pravnoj pomoći i o visokotehnološkom kriminalu smatraju se „najčešće" korišćenim instrumentima i, generalno, ocenjene su kao „adekvatne". Ipak, države ugovornice su identifikovale neke potencijalne nedostatke i oblasti u kojima bi se postojeće zakonodavstvo moglo poboljšati. Najvažniji nedostaci koji su primećeni odnose se na:

- Odsustvo zajednički dogovorenog (standardizovanog) pravnog okruženja koje podržava razmenu između pružalaca internet usluga i nadležnih organa kada se bave specifičnim istragama;
- Odredbe koje omogućavaju blagovremeni odgovor privatnih kompanija na zahteve za dostavljanje podataka;
- Odredbe kojima se primoravaju privatne kompanije da otkriju informacije na direktan zahtev/nalog druge države ugovornice;
- Odredbe kojima se sprovode zajednička pravila o čuvanju podataka;
- Odredbe za olakšavanje prikupljanja svedočenja žrtava i korišćenje svedočenja u drugoj državi;
- Pitanja u vezi sa transnacionalnim merama protiv veb lokacija na kojima se nalaze materijali koji se mogu povezati sa olakšavanjem eksploatacije žrtava;
- Odredbe koje uvode „obavezu stalnog praćenja" za kompanije u čitavom lancu snabdevanja;
- Upotrebu terminologije koja ne dozvoljava uvek da se zakonodavstvo razvija paralelno sa promenama u *modus operandiju* trgovaca ljudima;

- Razlike u prenošenju krivičnog dela trgovine ljudima (prema Protokolu UN iz Palerma) u nacionalno zakonodavstvo.

## Konvencija o visokotehnološkom kriminalu (Budimpeštanska konvencija) i borba protiv trgovine ljudima posredstvom IKT

Konvencija Saveta Evrope o sajber kriminalu (Budimpeštanska konvencija) je najrelevantniji instrument usmeren ka kriminalu posredstvom IKT koji navode države ugovornice.

Države ugovornice smatraju odredbe koje se odnose na **procesno pravo** najznačajnijim u kontekstu trgovine ljudima posredstvom IKT (Poglavlje II, odeljak 2. Konvencije). Štaviše, one su naglasile **značaj neograničavanja procesnih mera na ona krivična dela koja su izričito navedena** (npr. ona u Poglavlju II, odeljak 1.) Konvencija jasno ostvaruje svoj puni potencijal samo kada nije ograničena na krivična dela koja su izričito navedena u Poglavlju II, odeljak 1. Ovo je naročito tačno u kontekstu trgovine ljudima posredstvom IKT.

Nekoliko država je ukazalo na korisnost odredbi navedenih u Poglavlju III Konvencije o međunarodnoj saradnji kao pravnom osnovu za **prikupljanje i razmenu elektronskih dokaza** među državama. Konvencijom se uspostavlja mreža kontaktnih tačaka. Iako je ovo važan alat, gledajući u budućnost, verovatno je da će – sa sve centralnijom ulogom koju igraju IKT i elektronski dokazi – takve kontaktne tačke biti pod sve većim pritiskom – i brzo preopterećene ako ne budu imale adekvatno osoblje. Ovo nas dovodi do problema **uskih grla** unutar sistema, pri čemu je ključno odrediti gde se nalazi kontaktna tačka unutar sistema krivičnog pravosuđa, što može da bude veoma značajno.

Gledajući u budućnost, sledeći koraci mogu da omoguće da se **Konvencija o visokotehnološkom kriminalu dalje koristi** u borbi protiv trgovine ljudima:

- Sprovođenje Drugog dodatnog protokola uz Konvenciju, koji je usvojen u novembru 2021. godine i biće otvoren za potpisivanje 12. maja 2022. godine;
- Završetak usaglašavanja nacionalnog zakonodavstva sa Konvencijom o visokotehnološkom kriminalu kako bi se iskoristio njen pun potencijal;
- Šira i poboljšana obuka o mogućnostima koje nudi Konvencija o visokotehnološkom kriminalu pošto neke države ugovornice trenutno ne koriste raspoložive alate u njihovom punom potencijalu;
- Veća svest o obimu proceduralnih odredbi sadržanih u Konvenciji, pošto dokazi ukazuju na određeni stepen neslaganja među ispitanim državama o meri u kojoj se sadašnje odredbe mogu primeniti na slučajeve trgovine ljudima;
- Sprovođenje procedure za ubrzanje pružanja uzajamne pravne pomoći omogućavanjem slanja zahteva direktno subjektu koji se nalazi u stranoj državi, pod uslovom da je o tome obavešten pravosudni organ te države;
- Razvoj sinergije između GRETA i Komiteta za Konvenciju o visokotehnološkom kriminalu (TC-Y) radi kontinuiranog procenjivanja primene Konvencije o visokotehnološkom kriminalu u kontekstu trgovine ljudima.

## Izazovi koje su identifikovale NVO

NVO su ukazale na „jasna ograničenja" u pogledu **zaštite podataka (GDPR) i pravila privatnosti**. Osim toga, one pozivaju na donošenje zakona koji dozvoljavaju korišćenje **digitalne forenzike** kao prihvatljivog dokaza u svim državama. Dalji izazovi se odnose na ažuriranje propisa tako da uzimaju u obzir visokotehnološki (sajber) kriminal i internet, kao i osmišljavanje zakonodavstva i operativnih pravila za digitalne istrage.

## Nacionalni pravni okviri koji se odnose na uklanjanje sadržaja u vezi sa trgovinom ljudima

Velika većina država ima zakonske mere koje uređuju identifikaciju, filtriranje i uklanjanje internet sadržaja u vezi sa trgovinom ljudima. Mere se često ne odnose konkretno na trgovinu ljudima, već uopšteno na „nezakonit sadržaj" (izuzetak su materijali o seksualnoj eksploataciji dece). U nekim državama procedure za uklanjanje sadržaja u vezi sa trgovinom ljudima zahtevaju sudski nalog. Neke od ovih država smatraju ove procedure „suviše rigidnim" ili neefikasnim i zalažu se za efikasnija sredstva. Na kraju, neke države su naglasile da pružaoci usluga koji se nalaze u inostranstvu mogu lako da zaobiđu nacionalno zakonodavstvo o pravnoj odgovornosti pružalaca usluga.


## Ljudska prava, etika i zaštita podataka

### Dokazi prikupljeni od država ugovornica

Sve države ugovornice su navele usvajanje domaćeg zakonodavstva koje uređuje **obradu podataka** i **zaštitu podataka**. Što se tiče **lične zaštite žrtava**, jedan broj država je ukazao na uvođenje mera za sprečavanje počinilaca da stupe u kontakt sa žrtvama; ispitivanje svedoka putem video-konferencije kako bi se sprečio kontakt sa optuženima; a u nekim slučajevima i mogućnost da žrtve pruže dokaze na sudu anonimno radi zaštite njihovog identiteta.

Države ugovornice su navele da imaju uspostavljene **starosno osetljive protokole** u obliku različitih skupova procedura i zaštitnih mera koje se obično primenjuju u zavisnosti od toga da li je žrtva dete (mlađe od 18 godina). Što se tiče **rodno osetljivih protokola**, sve države kojima su ove informacije dostupne navele su da nemaju takve protokole, a jedini izuzetak je Austrija, koja je ukazala na poseban sistem podrške zasnovan na polu žrtve.

### Dokazi prikupljeni od NVO

U okviru standardne procedure, NVO traže pristanak žrtve pre nego što podele informacije sa organima za sprovođenje zakona. Problemi nastaju kada žrtve oklevaju da podnesu pritužbu policiji iz različitih razloga, uključujući rizik od odmazde, socijalnog isključenja ili mogućnost da žrtva bude deportovana. NVO procenjuju da je to slučaj sa „mnogim žrtvama trgovine ljudima". Pitanja zaštite podataka i razmene podataka mogu da stvore **moralne dileme**. Dok deljenje podataka sa organima za sprovođenje zakona i podnošenje pritužbi *podržava* istrage, koje potom kasnije mogu potencijalno spasiti i zaštititi više žrtava, to ima svoju cenu za pojedinačnu žrtvu, koja bi mogla biti izložena rizicima i pretnjama.

NVO su pozvale da se posveti više pažnje **potencijalnim rizicima i šteti koje stvaraju prikupljanje podataka velikih razmera i tehnološki alati**. Takođe su pozvali na dalje

razmatranje i dodatne mere kontrole korišćenja podataka i njihovog bezbednog čuvanja – i da se obezbedi poštovanje pravila zaštite podataka.

Na kraju, postoji veoma ograničen broj dokaza o **rodno osetljivim protokolima** koje su razvile NVO. **Starosno osetljivi protokoli** se obično primenjuju na osnovu toga da li je žrtva maloletna ili odrasla osoba.

## Dodatni dokazi prikupljeni na osnovu analize okruženja

IKT mogu da imaju značajan uticaj na **ljudska prava** pojedinaca, uključujući pravo na privatnost, slobodu izražavanja i zaštitu od diskriminacije. Politike za borbu protiv trgovine ljudima koje se u velikoj meri oslanjaju na tehnologiju moraju biti osmišljene tako da uzimaju u obzir ljudska prava.

Identifikovana su ključna pitanja koja se odnose na **privatnost podataka, etiku, transparentnost, odgovornost i informisani pristanak**. OEBS (2020) je identifikovao niz etičkih pitanja u vezi sa razvojem tehnologije za borbu protiv trgovine ljudima, uključujući: (a) zaštitu privatnosti podataka; (b) protokole o saglasnosti koje potpisuju žrtve; (c) obuku za osobe koje rukuju osetljivim podacima, posebno podacima o žrtvama; (d) bezbedno čuvanje podataka; (e) sprečavanje upotrebe tehnologije za prikupljanje osetljivih podataka o ranjivim osobama (na primer, opšte prikupljanje podataka o ranjivim ili marginalizovanim populacijama, čime se stvara rizik od diskriminatornih praksi); i (f) korišćenje tehnologije na način koji ne krši ljudska prava žrtava, kao ni prava opšte populacije. ICAT (2019) i drugi izvori ukazali su na osetljivost u vezi sa deljenjem podataka. Kada se podaci dele između država i/ili relevantnih agencija, to treba da se uradi u skladu sa načelima privatnosti i poverljivosti.

Gerry i drugi (2016) upozorili su na rizik koji donose široko rasprostranjeni **alati za praćenje** u borbi protiv trgovine ljudima. Iako takva tehnologija može da ponudi nove mogućnosti za intervenciju u situacijama trgovine ljudima, ona se takođe sastoji od **oblika nadzora koji potencijalno veoma zadire** u privatnost pojedinca.

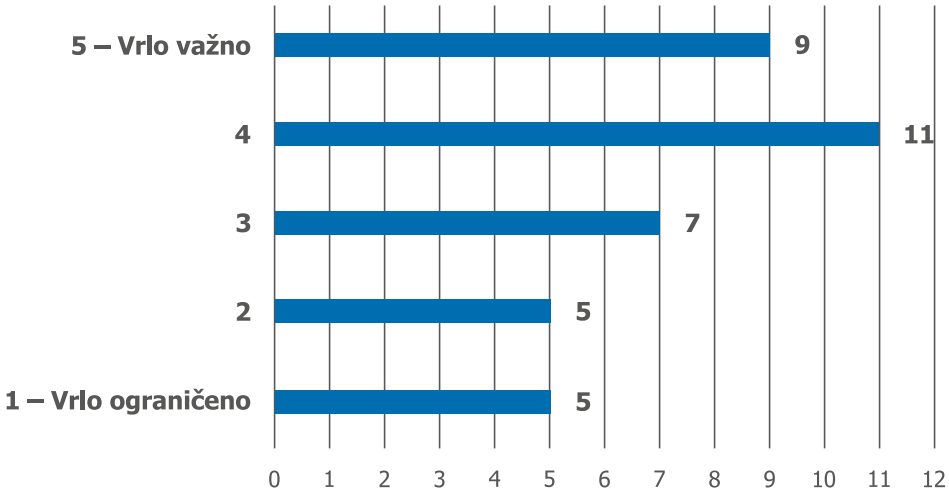
Na kraju, nekoliko izvora, uključujući Milivojević i drugi (2020) i Gerry i drugi (2016), ističe značaj **da se žrtvama ne uskraćuje mogućnosti korišćenja tehnologije**, jer pristup tehnologiji može biti njihov jedini način da komuniciraju sa spoljnim svetom i može da posluži kao važan mehanizam suočavanja. Uklanjanje pristupa tehnologiji može da obespravi žrtve; promovisanje bezbednog pristupa tehnologiji treba umesto toga da ima prednost. Uopšteno govoreći, najbolji interes žrtve treba da bude stavljen u centar svake akcije.

# 1. Uticaj tehnologije na trgovinu ljudima

## 1.1. Dokazi prikupljeni od država ugovornica

Dokazi koje su dostavile države ugovornice potvrđuju sve veći značaj tehnologije u kontekstu trgovine ljudima, a naročito u vezi sa regrutovanjem i eksploatacijom. Tehnologija i onlajn aktivnosti postaju sve relevantnije u životima ljudi – i to se ogleda u kontekstu trgovine ljudima. Većina država ugovornica smatra da je uticaj tehnologije na trgovinu ljudima „veoma važan" ili „važan" (slika 1).[4]

Slika 1. Uticaj tehnologije na trgovinu ljudima: Države ugovornice




Napomena: N = 37

Među državama koje su prijavile ograničen uticaj, neke su takođe prijavile veoma ograničene slučajeve ili nepostojanje slučajeva trgovine ljudima (tj. nizak tehnološki uticaj, opšti nizak nivo trgovine ljudima). U drugim državama, upotreba tehnologije je (još uvek) prilično ograničena (tj. niska upotreba tehnologije, nizak tehnološki uticaj). U ovom poslednjem slučaju, slika bi se mogla promeniti kako upotreba tehnologije postaje rasprostranjenija. Zaista, neke države ugovornice su istakle sve veći značaj onlajn materijala, reklama/oglasa i stranica/aplikacija za traženje posla, kao i **sve veći značaj** onlajn socijalizacije i ličnih interakcija. Sa druge strane, oba ova segmenta **stvaraju prilike** za počinioce u oblasti trgovine ljudima i **pogoršavaju postojeće ranjivosti.**

### 1.1.1. Trgovina ljudima u svrhu seksualne eksploatacije

U kontekstu **regrutovanja u svrhu seksualne eksploatacije**, nekoliko država ugovornica je identifikovalo slučajeve oglasa za posao koji nude sumnjivo visoke plate, često u sektorima usluga, što se pokazalo kao sredstvo za regrutovanje pojedinaca za eksploataciju. Nekoliko država je ukazalo na prisustvo veoma obmanjujućih ili potpuno lažnih oglasa za posao, koji su često objavljeni na veb lokacijama kojima se često pristupa i koji su navedeni među legitimnim oglasima. Pored toga, postoje dokazi o regrutovanju preko platformi društvenih medija od strane pojedinaca koji nude poslove, na primer, u ugostiteljstvu (npr. konobarisanje) i poljoprivredi. Počinioci obično obećavaju (nepostojeći) dobro plaćen posao u inostranstvu, a zatim prisiljavaju osobu da pruža seksualne usluge u zemlji odredišta.

4 Tri države nisu dale odgovor na ovo pitanje.

Prema Nacionalnom izveštaju o situaciji u vezi sa trgovinom ljudima za 2019. godinu koji su pripremile nemački nadležni organi, 11% identifikovanih žrtava kontaktirano je ili regrutovano putem interneta (N = 47). Od tih 47 žrtava, 31 je kontaktirano preko često korišćene platforme društvenih medija, a 13 preko portala za oglašavanje (tri žrtve su regrutovane korišćenjem „druge" metode zasnovane na internetu). Bugarska nacionalna komisija za borbu protiv trgovine ljudima istakla je da su potencijalne žrtve koje se kontaktiraju putem društvenih medija „uglavnom mlade devojke i žene". Holandske vlasti su prijavile da se, na osnovu informacija dostupnih u policijskom sistemu, platforme društvenih medija koriste za regrutovanje maloletnih žrtava. Prema dokazima iz Austrije, regrutovanje se obično odvija u državama porekla žrtava.

Kada se obraćaju potencijalnim žrtvama na internetu, počinioci mogu da primenjuju prilično sofisticiran *modus operandi*, često zasnovan na lažnim profilima koji pokazuju visok životni standard i značajno bogatstvo. Kako su navele bugarski nadležni organi, „određeni broj istraga je otkrio da pre nego što priđu svojim potencijalnim žrtvama i započnu regrutovanje, počinioci pažljivo pregledaju fotografije svojih meta [kako bi] istražili njihove životne uslove, društveni status i okruženje, porodične odnose i status veze, kao što su brak, razvod ili veridba. […] Tek nakon tako pažljivog ispitivanja počinioci stupaju u kontakt sa svojim žrtvama, koristeći izuzetne psihološke veštine ubeđivanja i motivisanja žrtava da se upuste u određena ponašanja". Dokazi o takvom *modus operandiju* opsežni su i dolaze iz nekoliko zemalja, uključujući Austriju, Bosnu i Hercegovinu, Bugarsku, Belgiju, Hrvatsku, Mađarsku, Republiku Moldaviju, Holandiju, Poljsku, Portugal, Slovačku, Švedsku i Ukrajinu. Takav *modus operandi* je često deo takozvane tehnike „ljubavnika", tj. pretvaranja da se počinilac upušta u romantičnu vezu kako bi se žrtva primorala na prostituciju. Kako su ocenili nadležni organi u Rumuniji, između ostalih, „tehnika ljubavnika je i dalje najčešće korišćeno sredstvo". Sastoji se u kontaktiranju osobe preko onlajn platforme, upoznavanju njenih hobija i interesovanja, porodične situacije i ličnih okolnosti (kao i ranjivosti). Nakon toga, „trgovac ljudima prilazi žrtvi sa empatijom, sa velikom željom da joj pomogne i da je razume, kao i da je finansijski podrži. Često se žrtvom manipuliše obećanjima ozbiljne veze, ponekad i zahtevima za brak, u pokušaju da se zadobije njeno poverenje, a zatim i kako bi se uspostavila psihološka kontrola nad žrtvom" (dokazi iz Rumunije). Prema dokazima iz Belgije, žrtve regrutovane preko platformi društvenih medija imaju tendenciju da pokazuju obrasce porodične nestabilnosti, napuštanja škole, niskog samopoštovanja i, uopšteno, psihosocijalne ranjivosti.

Dokazi iz Francuske ukazuju da mreže trgovine ljudima različitih nacionalnosti, uključujući južnoameričkim, istočnoevropskim i francuskim državljanima uključenim u takozvanu trgovinu ljudima „*de cité*" („podvođenje u uskraćenom kraju") koriste društvene mreže za regrutovanje žrtava. Čini se da su mreže za trgovinu ljudima koje uključuju pojedince iz afričkih zemalja izuzetak od ovog pravila. Brojne države su dostavile dokaze o regrutovanju preko aplikacija za upoznavanje (uključujući Ujedinjeno Kraljevstvo, Norvešku, Finsku, Austriju, Ukrajinu i Belorusiju).

Dostupno je obilje dokaza iz više zemalja o slučajevima **ucene**. Ovo se najčešće postiže time što se prvo prikupe „kompromitujuće" informacije o žrtvama – na primer, time što se traže fotografije ili video-snimci nagog tela – i potom koriste te informacije da se osoba prisili na prostituciju. Počinioci prvo uspostavljaju odnos sa žrtvom, zadobijaju njeno poverenje, a zatim traže „kompromitujuće" informacije. Nekoliko država ugovornica prijavilo je dokaze takvog ponašanja, uključujući Bosnu i Hercegovinu, Bugarsku, Hrvatsku, Holandiju, Finsku, Litvaniju i Švedsku.

Neke države su navele primere žrtava koje su regrutovane na internetu među pojedincima voljnim da pružaju seksualne usluge; međutim, nakon regrutovanja bivaju izložene eksploatišućem

radnom vremenu i veoma lošim uslovima smeštaja, i suočene su sa mogućnostima zarade koje se drastično razlikuju od onih koje se oglašavaju (dokazi iz Mađarske i Poljske). Dokazi iz Poljske takođe ukazuju na slučajeve žena koje reklamiraju seksualne usluge a koje su na meti trgovaca ljudima, zastrašivane i primorane da dele svoj profit (mehanizam sličan iznudi).

Postoje brojni dokazi iz nekoliko država o internet stranicama koji se koriste za **oglašavanje seksualnih usluga**. U okviru takvih oglasa nalaze se i oglasi povezani sa uslugama koje pružaju žrtve trgovine ljudima. Kako su napomenule britanski nadležni organi, veb lokacije za usluge za odrasle (ASW) „su i dalje najznačajniji **omogućavač seksualne eksploatacije** povezane sa trgovinom ljudima u Ujedinjenom Kraljevstvu". ASW lokacije su „privlačne za počinioce jer često zahtevaju malo verifikacije korisnika i omogućavaju pristup velikoj bazi potencijalnih klijenata" (prijava britanskih nadležnih organa). Prema dokazima iz Finske, „IKT platforme, naročito stranice za oglašavanje zasnovane na forumima, su glavni modus operandi kada je reč o marketingu i kontaktiranju klijenata u kontekstu trgovine ljudima". Francuski nadležni organi navode da je internet koristilo 65% identifikovanih žrtava seksualne eksploatacije tokom 2019. godine; ovo je povećanje u odnosu na 49% u prethodnoj godini. Jedno od ključnih pitanja koje su britanski nadležni organi istakli u prijavi – a koje se primećuje i kod drugih – jeste da se „oglasima koje objavljuju trgovci ljudima daje legitimitet njihovim pojavljivanjem pored oglasa koje objavljuju autonomni seksualni radnici". Prema nadležnim organima u Finskoj, „žrtve trgovine ljudima i seksualni radnici koje nisu žrtve koriste iste stranice". Nadležnim organima često predstavlja izazov da razvrstaju oglase povezane sa trgovinom ljudima od onih koje objavljuju nezavisni seksualni radnici (videti takođe Poglavlje 2).

Tehnologija se može koristiti za **koordinaciju aktivnosti tokom faze eksploatacije**, kao i za uspostavljanje kontakta sa potencijalnim klijentima (uključujući pregovaranje o cenama, određivanje lokacija i sklapanje dogovora). Ono što je ključno je da tehnologija omogućava **razdvajanje** između mesta gde se seksualna aktivnost izvodi i mesta gde se vrši koordinacija. Ovo ima važne implikacije u pogledu sprovođenja zakona. Na primer, nadležni organi Bosne i Hercegovine su izneli dokaze o lancu koji eksploatiše žene iz Bosne koje pružaju seksualne usluge u Nemačkoj i Austriji – tim uslugama su koordinirali i upravljali počinioci sa sedištem u Bosni i Hercegovini. Ovo uključuje aktivnosti kao što je upravljanje onlajn profilima žrtava i zakazivanje sastanaka sa klijentima. Dokazi iz Francuske ukazuju na prisustvo platformi za upravljanje pozivima i upravljanje sastancima na daljinu sa Kipra (za mreže na ruskom govornom području) i iz Kine (za mreže na kineskom govornom području). U brojnim slučajevima koje je švedska policija analizirala tokom 2019. godine, postojale su „sumnje da su aktivnosti prostitucije organizovane od strane kriminalnih mreža sa sedištem u državama porekla žena ili kroz povezanost sa agencijom u trećoj državi". U istom izveštaju su takođe identifikovane slike različitih žena koje su povezane sa istim ili veoma sličnim adresama e-pošte i/ili istim brojevima mobilnih telefona. Nadležni organi su ovo protumačili kao indikatore znakova upozorenja. Švedski nadležni organi su takođe naišli na slučajeve nepismenih Nigerijki i Rumunki koje su imale profil na ASW. Ovo ukazuje na to da je takve profile izradio i njima upravljao neko drugi – još jedan potencijalni znak upozorenja.

Države su pružile dokaze o tehnološkim alatima koje trgovci ljudima koriste za **praćenje i kontrolu žrtava** tokom faze eksploatacije. U slučaju koji su prijavile slovenački nadležni organi, trgovci ljudima su tražili od žrtava da putem interneta prijave svaku pruženu uslugu. Žrtve su takođe morale da prijave druge žrtve kako bi trgovci ljudima imali potpunu kontrolu nad njihovim aktivnostima. U drugim slučajevima, određene aplikacije su korišćene za praćenje lokacije žrtve.

Na kraju, pored dve „glavne" oblasti regrutovanja i eksploatacije, postoje dokazi da se tehnologija koristi kao pomoćno sredstvo logistike trgovine ljudima, uključujući kupovinu avionskih

karata, kao i, u nekim slučajevima, pribavljanje lažnih putnih i drugih isprava (dokazi sa Kipra). Aplikacije i veb lokacije se takođe mogu koristiti za rezervisanje nekretnina u kojima se pružaju seksualne usluge (dokazi iz Francuske, Estonije, Ujedinjenog Kraljevstva i Španije). Iako su deo trgovine ljudima, takve aktivnosti su pomoćne uz dve osnovne aktivnosti regrutovanja i eksploatacije.

Kao **trendovi u nastajanju** u kontekstu seksualne eksploatacije primetan je porast slučajeva **emitovanja uživo** seksualnih aktivnosti koje izvode žrtve trgovine ljudima. Iako je emitovanje uživo često povezano sa seksualnim zlostavljanjem dece, više država je ukazalo na činjenicu da emitovanje uživo može takođe da uključuje i odrasle žrtve trgovine ljudima. Kiparski nadležni organi su primetili sve češće korišćenje veb kamera za prenos uživo. Prema španskim nadležnim organima, trgovci ljudima „sve više" koriste veb stranice za emitovanje video zapisa kako bi plasirali usluge koje pružaju žrtve trgovine ljudima. Slično tome, irski nadležni organi su primetili brz porast takozvanih aplikacija za video ćaskanje po principu „plati koliko koristiš", kao što su Escortfans i Onlyfans, koje zamenjuju tradicionalne veb platforme pružajući mogućnost za gledanje pratnje u onlajn prostorijama za privatno ili javno ćaskanje. Irski nadležni organi su tvrdili da je „priroda ovih aplikacija i veb lokacija učinila gotovo nemogućim da se sazna da li neko dobrovoljno koristi platforme ili trpi eksploataciju" (sličan trend je primećen i u Finskoj). Ovaj segment tržišta se navodno „eksponencijalno proširio" od izbijanja pandemije kovida-19. Kako su napomenuli holandski nadležni organi, „očekuje se da će se broj platformi još više povećati u (skoroj) budućnosti". Ovaj trend se proteže i na stranice i aplikacije za upoznavanje, veb stranice za oglašavanje seksualnih usluga, kao i na društvene medije koji se primarno ne fokusiraju na seksualne usluge, ali se mogu koristiti u tu svrhu.

Kiparski nadležni organi su takođe primetili povećanje upotrebe aplikacija za kontrolu žrtava, npr. korišćenje automatizovanih poruka koje se šalju na mobilni telefon trgovca ljudima svaki put kada žrtva izvrši određenu radnju (npr. otvori ulazna vrata). Švajcarski nadležni organi su slično tome ukazali na otkrivanje aplikacija za lociranje na telefonima žrtava, koje su verovatno instalirane bez njihovog znanja. Sličan trend korišćenja tehnologije za kontrolu žrtava primećen je i u Austriji. Pored toga, grčki nadležni organi su prijavili porast broja slučajeva regrutovanja dece migranata putem mobilnih tehnologija u svrhu seksualne eksploatacije.

Nekoliko država je prijavilo **povećanje onlajn interakcija** zbog pandemije kovida-19, čime se povećavaju mogućnosti za trgovce ljudima da uspostave kontakt sa ranjivim pojedincima. Rumunski nadležni organi su primetili porast broja žrtava koje su regrutovane putem interneta tokom poslednjih godina, a naročito nakon mera za zaštitu javnog zdravlja zbog kovida-19. Međutim, kao što navode, u Rumuniji se većina žrtava i dalje regrutuje putem direktnog kontakta sa prijateljima, partnerima i rođacima. U Francuskoj, nadležni organi su primetili prelazak sa ulične ponude na „diskretniji" sistem zasnovan na oglasima na internetu nakon usvajanja Zakona od 13. aprila 2016. godine koji kriminalizuje kupovinu seksualnih usluga. Oni su takođe primetili ubrzanje ovog procesa nakon pandemije kovida-19. Prema švedskom tužilaštvu, upotreba interneta u vezi sa trgovinom ljudima u seksualne svrhe je toliko rasprostranjena da sada „teško da postoji slučaj trgovine ljudima u kojem se internet ne pojavljuje" kao deo *modus operandija* trgovaca ljudima. Belgijski nadležni organi očekuju porast broja slučajeva ranjive dece ili mladih odraslih koji su regrutovani posredstvom IKT u svrhu seksualne eksploatacije – pošto ljudi u ovim starosnim grupama sve više komuniciraju onlajn i putem IKT (u tehnološkom okruženju koje se stalno menja i koje predstavlja izazov za aktivnosti istražitelja).

### 1.1.2. Trgovina ljudima u svrhu radne eksploatacije

Dokazi koje su pružile države ugovornice pokazuju da se, u kontekstu trgovine ljudima u svrhu radne eksploatacije, IKT uglavnom koriste za **regrutovanje** žrtava. Prema tvrdnjama nemačkih nadležnih organa, internet i društveni mediji igraju „sve važniju ulogu u uspostavljanju kontakata i regrutovanju u oblasti trgovine ljudima i radne eksploatacije". Ovo mišljenje dele i španski nadležni organi, prema kojima onlajn regrutovanje u svrhu radne eksploatacije „postaje sve rasprostranjenije". Ovaj proces je verovatno ubrzao kovid-19 i posledični rast prostora na internetu koji zamenjuju interakcije licem u lice i sastanke. Kako su istakli irski nadležni organi, „ova sve veća upotreba društvenih medija za regrutovanje radnika migranata predstavlja sve veći izazov za organe koje se bore protiv obmanjujućeg i eksploatativnog regrutovanja na mreži". Prema francuskim nadležnim organima, iako se čini da „tradicionalni oblici zapošljavanja (oglasi u novinskim rubrikama za zapošljavanje, mali oglasi, flajeri, usmene preporuke itd.) i dalje preovlađuju, upotreba oglasa na internetu je sve rasprostranjenija". Ovo je povezano sa velikim porastom upotrebe IKT-a od strane onih koji traže posao.

Dokaze o **obmanjujućim/lažnim oglasima za posao** u kontekstu regrutovanja u svrhu radne eksploatacije pružilo je više država, uključujući Austriju, Hrvatsku, Kipar, Estoniju, Finsku, Francusku, Grčku, Letoniju, Litvaniju, Republiku Moldaviju, Norvešku, Poljsku, Portugal, Rumuniju, Švedsku i Švajcarsku. Bugarski nadležni organi su istakli prisustvo oglasa na raznim stranicama za traženje posla u kojima „poslodavac" obećava velike plate, besplatan prevoz, besplatan smeštaj i bonuse za poslove koji ne zahtevaju razvijene veštine ili tečno poznavanje lokalnog jezika. Takvi oglasi su često deo *modus operandija* trgovaca ljudima koji žele da regrutuju radnike koji bi potom radili u uslovima eksploatacije. Ovo se može primetiti i u dokazima koje su pružili nemački nadležni organi, prema kojima „neki počinioci u početku nude zaposlenje na raznim internet portalima. Poslovi bi trebalo da budu dobro plaćeni, a radno vreme je navodno uređeno". Međutim, po dolasku u Nemačku, radnici „nisu dobili zvaničan ugovor o radu, niti su plaćeni kao što im je obećano. Često ne primaju nikakvu zaradu ili dobijaju samo delić obećane naknade". Slični oglasi su primećeni i u Španiji, gde se „mnoge žrtve trgovine ljudima u svrhu radne eksploatacije regrutuju preko internet stranica za oglašavanje", navode nadležni organi.

Postoje dokazi iz Ujedinjenog Kraljevstva o lažnim oglasima za zapošljavanje koji su kružili društvenim medijima koji promovišu mogućnosti zapošljavanja za visoko plaćenu radnu snagu/građevinarstvo u Londonu – u stvarnosti, kako su istakli nadležni organi, „ovo često nije slučaj i posao ne postoji". Što se tiče sadržaja oglasa, britanski nadležni organi su napomenuli da je „većina oglasa za posao koje su koristili trgovci ljudima zasnovana na nejasnim obećanjima o dobrom poslu, visokim zaradama i dobrim uslovima, bez navođenja konkretnih oblika rada ili visine zarade. Međutim, u manjini zabeleženih slučajeva, oglasi za posao su ipak sadržali ove detalje. Kod radne eksploatacije, više nego kod seksualne eksploatacije, uobičajeno je da se opiše sektor rada, iako se takođe redovno prijavljuju obmane". Počinioci ulažu velike napore da naizgled stvore legitimitet iza kojeg mogu da sakriju svoju pravu prirodu: „Počinioci koji poseduju kompanije u kojima se vrši eksploatacija takođe koriste internet omogućivače koji odražavaju legitimne operatere na istom tržištu, koriste imenike usluga i usluge mapiranja da bi istakli radno vreme i usluge koje se nude" (dokazi iz Ujedinjenog Kraljevstva). Postoje dokazi iz više država koji ukazuju na to da se oglasi/reklame obično postavljaju na „poznate veb stranice za oglašavanje", kako u državi porekla žrtve (dokazi iz Litvanije), tako i u državi eksploatacije (dokazi iz Francuske i Grčke). Drugi *modus operandi*, opisan u prijavi britanskih nadležnih organa, sastoji se od toga da počinioci koriste „internet platforme da identifikuju

uloge ili slobodna radna mesta na kojima će žrtve biti zaposlene i otvaraju bankovne račune za primanje zarada" (ovo je tzv. „model ne-poslodavca").

Različite države mogu da tumače trgovinu ljudima u svrhu radne eksploatacije na različite načine, a granice između trgovine ljudima, zloupotrebe rada i nepoštovanja propisa mogu biti zamagljene i mogu da variraju od države do države (konceptualno, one se mogu kretati u rasponu ozbiljnosti od nepoštovanja propisa do situacija u kojima se oduzimaju pasoši i ozbiljno ograničava sloboda kretanja). Na primer, britanski nadležni organi su primetili da neki oglasi otvoreno upućuju na visine zarada koje su ispod nacionalne minimalne zarade; međutim, „velika je verovatnoća da se ovi [oglasi] odnose na zloupotrebe na radu i nepoštovanje propisa, a ne na trgovinu ljudima". Trgovci ljudima mogu da „izbegnu prihvatanje obaveze isplate bilo kog iznosa, što takođe smanjuje potencijal da privuku pažnju organa za sprovođenje zakona i regulatornih organa". Ovo još jednom ukazuje na poteškoće sa kojima se nadležni organi suočavaju prilikom identifikovanja i uklanjanja takvih oglasa.

Oglasi se ne objavljuju samo na veb lokacijama za male oglase za zapošljavanje, već se objavljuju i distribuiraju na društvenim medijima, na primer u **specijalizovanim grupama za traženje posla i grupama za uzajamnu pomoć** (npr. „Bugari koji žive u inostranstvu" ili „Nguoi tim viec", što znači „ljudi u potrazi za poslom" na vijetnamskom jeziku). Nekoliko država je istaklo značaj stranica koje imaju za cilj da podstaknu razmenu informacija među radnicima migrantima kao prostora za regrutovanje na meti trgovaca ljudima – prostora koji je često loše regulisan jer takve stranice mogu da vode pojedinci ili udruženja sa nedovoljnim resursima. U nekim slučajevima, takvi oglasi se mogu širiti preko grupa za traženje posla kreiranih u aplikacijama za razmenu poruka kao što je Telegram.

Oglasi mogu da sadrže veoma obmanjujuće informacije o uslovima rada i naknadama, a često i mogućnost kontaktiranja „poslodavca" ili „agencije" samo preko šifrovanih aplikacija kao što su Viber ili WhatsApp. Takve objave mogu da dođu do široke publike uz veoma male (ili nikakve) troškove. U društvenom eksperimentu, NVO iz Bugarske objavila je oglas za posao na Facebook stranici nudeći posao u Danskoj u „berbi zelene srne" (igra rečima koja potiče od bugarskog idioma „poslati nekoga po zelenu srnu", što znači poslati nekoga u uzaludnu potragu), uz izuzetno visoku zaradu po satu. Za manje od nedelju dana, više od 150 kandidata je dostavilo svoje biografije. Kao što je navedeno u nekoliko prijava, nivo tehničkih veština potrebnih za korišćenje onlajn resursa i društvenih medija u svrhu trgovine ljudima je relativno skroman i sličan je veštinama koje većina korisnika interneta obično poseduje (uzgred govoreći, ovo je daleko od nivoa sofisticiranih hakera i sajber kriminalaca).

Prema dokazima iz Bugarske, oglasi se često odnose na poslove u poljoprivredi (sezonski radnici), na gradilištima, u fabrikama i u ugostiteljskom sektoru. Ostali sektori koji se smatraju ugroženim su usluge u domaćinstvu i usluge nege. Nemački nadležni organi su identifikovali oglašavanje putem interneta u sledećim sektorima kao rizično: sezonski poljoprivredni radovi, usluge čišćenja, etno restorani, građevinarstvo, prehrambena industrija, transport i lepota (saloni za nokte i masažu). Portugalski nadležni organi su prijavili nekoliko slučajeva koji su povezani sa veoma obmanjujućim/lažnim oglasima za poslove u sektoru poljoprivrede i građevinarstva. Švedski nadležni organi su označili usluge čišćenja, građevinarstvo, restorane i salone za nokte. Osim toga, kiparski nadležni organi su označili ponude lažnih obrazovnih mogućnosti na privatnim univerzitetima i koledžima.

Kao **trend u nastajanju** u kontekstu radne eksploatacije, bugarski nadležni organi su prijavili porast slučajeva regrutovanja putem interneta i društvenih mreža. Veruje se da je

ovo ubrzano izbijanjem kovida-19 i povezanim merama za zaštitu javnog zdravlja. Slično povećanje broja oglasa na društvenim mrežama su, između ostalih, primetili kiparski, nemački i francuski nadležni organi. U Francuskoj su nadležni organi počeli da primećuju korišćenje grupa za samopomoć u zajednici za regrutovanje i kontrolu žrtava i za prenose sredstava. Na kraju, Francuska i Ujedinjeno Kraljevstvo su ukazali na povećanje mogućnosti za iskorišćavanje žrtava povezanih sa „ekonomijom honorarnih poslova", pošto se identifikacioni dokumenti ne proveravaju redovno i pojedinci mogu da rade na tuđ račun. Na primer, treća strana može da primi sve zarade na svoj bankovni račun i da samo manji deo prenese na radnika. Prema britanskim nadležnim organima, „ovaj *modus operandi* je identifikovan kao tehnika koja omogućava zloupotrebe na radu i rad na crno, dok nivo kontrole koji vlasnik računa ima nad finansijama radnika predstavlja rizik od trgovine ljudima". Ovo gledište dele i francuski nadležni organi, koji su primetili da „iako za sada nije zvanično otkriven nijedan slučaj trgovine ljudima, za neke samozaposlene radnike se smatra da organizuju oblike eksploatacije tako što daju u podzakup svoj račun neregularnim migrantima, terajući ih da rade bez zarade ili sa veoma malom zaradom". Na kraju, belgijski nadležni organi su primetili da je moguće nabaviti falsifikovane dokumente u grupama koje oglašavaju svoje usluge putem šifrovanih aplikacija za komunikaciju; takvi dokumenti se onda mogu koristiti za omogućavanje radne eksploatacije (npr. falsifikovane lične isprave i vozačke dozvole, lažni ugovori o radu i lažne radne dozvole).

### 1.1.3. Mračna mreža i kriptovalute

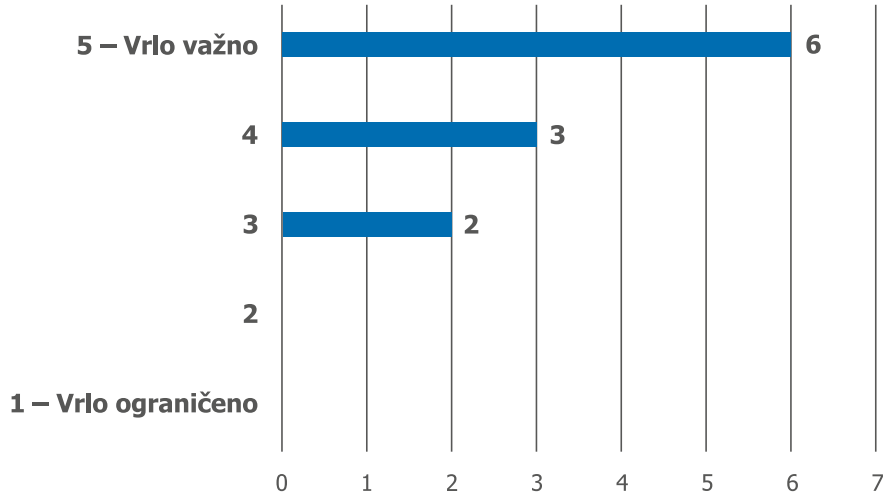
Sve u svemu, države ugovornice nisu prijavile nikakve dokaze o značajnoj upotrebi mračne mreže u kontekstu trgovine ljudima. Ograničeni izneti dokazi odnose se samo na širenje materijala o seksualnom zlostavljanju dece. Postoje neki dokazi iz Francuske da trgovci ljudima kupuju podatke o kreditnim karticama na mračnoj mreži, a zatim ih koriste za rezervisanje soba u hotelima i apartmanima za iznajmljivanje – međutim, čini se da je ova aktivnost prilično ograničena i pomoćna. Norveški i francuski nadležni organi su primetili da se seksualno zlostavljanje prenosi uživo na mračnoj mreži, ali iz pruženih dokaza nije jasno da li ovi prenosi uživo uključuju uglavnom decu ili takođe uključuju i odrasle žrtve. Sve u svemu, vrlo je verovatno da mračna mreža igra veoma ograničenu ulogu u ovom trenutku, pošto i tokom regrutovanja i eksploatacije trgovci ljudima nastoje da dopru do najšire moguće publike – a to je teško usaglasiti sa mračnom mrežom u njenom trenutnom uređenju i nivou korišćenja. Platforme sa velikim brojem korisnika su poželjnije za regrutovanje (zaista, jedna od ključnih prednosti tehnologije je mogućnost da se dopre do velike grupe pojedinaca uz relativno male troškove). Slično tome, oglasi za seksualne usluge na internetu zahtevaju kontakt sa širom publikom – nešto što nije moguće u tajnovitijoj mračnoj mreži.

Čini se da korišćenje kriptovaluta nije rasprostranjeno u kontekstu trgovine ljudima (sa druge strane, postoje dokazi o njihovoj upotrebi za kupovinu prenosa seksualnog zlostavljanja dece uživo na mračnoj mreži). Prenosi novca se i dalje obavljaju tradicionalnim metodama, npr. preko kompanija kao što su Western Union ili MoneyGram ili, u nekim slučajevima, korišćenjem pojedinaca (takozvanih „mazgi"). U nekim slučajevima mogu se koristiti neformalni sistemi za prenos novca, kao što je Hawala. Neke države su počele da prijavljuju prenose novca putem aplikacija za razmenu poruka (npr. WeChat). Verovatno je da će finansijsko-tehnološki proizvodi, npr. prenosi novca preko aplikacija, igrati sve veću ulogu u budućnosti – jer razvijaju veći otisak u širem društvu (slično važi za kriptovalute, kada – i ako – postignu veći opticaj). Konačno, postoje dokazi o korišćenju kartica i vaučera koji ne sadrže lične podatke (kao što su PaySafe kartice) za plaćanje onlajn usluga, npr. za kupovinu oglasnih prostora na veb stranicama za usluge za odrasle.

## 1.2. Dokazi prikupljeni od NVO

Tri od četiri NVO koje su konsultovane za potrebe izrade ove studije smatraju da je uticaj tehnologije na trgovinu ljudima „veoma važan" ili „važan", pri čemu nijedna NVO ne ukazuje na „ograničen" ili „veoma ograničen" uticaj (slika 2).[5]

Slika 2. Uticaj tehnologije na trgovinu ljudima: NVO




Napomena: N = 11

Sve u svemu, kvalitativni dokazi koje su dostavile NVO koje direktno pružaju pomoć žrtvama trgovine ljudima daju sličnu sliku kao dokazi koje su pružile države ugovornice. NVO su primetile korišćenje interneta i društvenih medija u svim fazama trgovine ljudima, a naročito u vezi sa (a) regrutovanjem; (b) eksploatacijom; i (c) vršenjem kontrole i pritiska nad žrtvama.

Među NVO preovlađuje mišljenje da se uticaj tehnologije na trgovinu ljudima povećao tokom pandemije kovida-19. Međutim, pandemija je možda samo ubrzala već postojeći trend. Kako je primetila KOK – nemačka mreža koja okuplja 37 NVO koje pružaju specijalizovane usluge savetovanja za žrtve trgovine ljudima – „već nekoliko godina savetovališta izveštavaju o sve većoj ulozi interneta i društvenih medija u trgovini ljudima".

Članovi La Strada International, evropske NVO platforme koja okuplja 30 organizacija za borbu protiv trgovine ljudima u 23 evropske države, prijavili su slučajeve trgovine ljudima koji su regrutovani putem različitih onlajn platformi, uključujući društvene medije i veb stranice za upoznavanje, kako u svrhu seksualne, tako i u svrhu radne eksploatacije. Ovi slučajevi su se ticali regrutovanja i odraslih i dece. Prema podacima koje je pružila CKM, NVO iz Holandije, onlajn kontakti igraju naročito važnu ulogu kada se žrtve i počinioci međusobno ne poznaju: u skoro 80% ovih slučajeva prvi kontakt se ostvaruje onlajn, npr. putem društvenih medija ili aplikacija za upoznavanje (dokaze pružila La Strada International). Ovo je naročito izraženo kod maloletnih žrtava. Na osnovu intervjua sa žrtvama trgovine ljudima, albanska NVO „Different and Equal" primetila je da su društveni mediji „postali glavno sredstvo" preko kojeg počinioci regrutuju žrtve. Ovo je naročito slučaj sa „devojčicama [regrutovanim] u svrhu seksualne eksploatacije". U Švajcarskoj, FIZ je takođe primetio novi trend regrutovanja u svrhu trgovine ljudima putem različitih platformi društvenih medija, kao i aplikacija za upoznavanje.

5 Jedna NVO nije dala odgovor na ovo pitanje.

Uopšteno posmatrano, postoji opšta saglasnost o činjenici da je upotreba – i značaj – tehnologije u slučajevima trgovine ljudima u porastu – i da se takva uzlazna putanja ubrzala tokom poslednjih godina.

### 1.2.1. Trgovina ljudima u svrhu seksualne eksploatacije

Strategije i mehanizmi koji predstavljaju osnovu za regrutaciju putem društvenih medija o kojima izveštavaju NVO u skladu su sa dokazima o kojima je već bilo reči u odeljku 1.1.1 iznad. Postoje dokazi o takozvanoj strategiji „ljubavnika", odnosno uspostavljanju lične/romantične veze putem društvenih medija kako bi se žrtva kasnije podvrgla eksploataciji. U tu svrhu se koriste lažni profili na društvenim medijima. Žrtve su obično maloletne ili mlade odrasle osobe. La Strada Moldova je istakla da su posebno ugrožena deca iz ruralnih područja, iz socijalno ugroženih porodica ili deca u lošoj materijalnoj situaciji.

NVO su istakle mehanizme slične onima o kojima je bilo reči ranije u ovom izveštaju u vezi sa fazom eksploatacije. Oni uključuju korišćenje veb lokacija za oglašavanje seksualnih usluga. Organizacija KOK (Nemačka) je primetila da je policiji i savetodavnim službama teže da priđu pojedincima koji oglašavaju seksualne usluge na internetu u odnosu na one koji pružaju iste usluge u registrovanim ustanovama – što čini identifikaciju slučajeva trgovine ljudima težom.

Dalje, u slučaju seksualne eksploatacije, smeštaj se može rezervisati onlajn preko specijalizovanih stranica (dokazi iz Francuske dobijeni od La Strada International).

### 1.2.2. Trgovina ljudima u svrhu radne eksploatacije

Što se tiče regrutovanja u svrhu radne eksploatacije, NVO su pružile dodatne dokaze za mehanizme o kojima je već bilo reči u odeljku 1.2.2 iznad, naročito o korišćenju lažnih i grubo obmanjujućih oglasa za posao na internetu. Na primer, u Albaniji je NVO „Different and Equal" primetila onlajn oglase za posao koji su povezani sa eksploatatorskim praksama usmerenim i na muškarce i na žene. U Srbiji je NVO „Astra" izrazila zabrinutost da bi čak i agencije koje su zvanično registrovane pri Agenciji za privredne registre i sa redovnom licencom mogle da oglašavaju nezakonite poslove. Takođe su primetili „velik broj" „neovlašćenih" oglasa, odnosno oglasa pojedinaca za koje se tvrdilo da su predstavnici agencija, kao i oglasa koji su povezani sa eksploatatorskim praksama. Većina oglasa na internetu, smatraju oni, „ne podleže nikakvom obliku kontrole ili nadzora". Nemačke i švajcarske NVO otkrile su i dokaze o regrutovanju putem interneta za poslove koji ili ne postoje ili su podložni uslovima eksploatacije. Ovo postoji u kontekstu „proliferacije regrutovanja za poslove putem interneta", kako je istakla organizacija Migrant Right Centre Ireland.

U prijavama NVO nema dokaza da tehnologija igra ključnu ulogu tokom faze eksploatacije u kontekstu radne eksploatacije. Međutim, naglašeno je da poslovi u ekonomiji honorarnih poslova, a naročito onlajn platforme za hranu i druge isporuke, mogu biti podložni zloupotrebi od strane trgovaca ljudima. Kako je primetila francuska NVO „*Comite Contre l'Esclavage Moderne*" (CCEM, francuska članica La Strada International), iako do sada nije identifikovan nijedan slučaj trgovine ljudima u ovom kontekstu, procedure koje trenutno primenjuju onlajn platforme za isporuku mogu da omoguće trgovcima ljudima da zapošljavaju žrtve koristeći tuđi identitet.

### 1.2.3. Kontrola i pritisak nad žrtvama

NVO su primetile da se tehnologija koristi za **vršenje kontrole nad žrtvama**, naročito u kontekstu seksualne eksploatacije. Bilo je slučajeva u kojima su se trgovci ljudima oslanjali na video nadzor, mobilne telefone, aplikacije i softvere za praćenje lokacije (dokazi koje je pružila La Strada International). Počinioci takođe mogu da koriste IKT za pretnje porodici i prijateljima, npr. putem društvenih medija, ako žrtva odluči da pobegne iz situacije u kojoj se nalazi (dokazi koje je pružio KOK, Nemačka). Slične dokaze prikupila je i NVO „Astrée" u Švajcarskoj.

Osim toga, žrtve mogu biti predmet **ucena** putem društvenih medija i drugih onlajn platformi. Ovo je često povezano sa pretnjom otkrivanja „kompromitujućih" informacija, uključujući fotografije i druge lične podatke (KOK izveštava o slučaju trgovca ljudima koji je ucenjivao svoju žrtvu preteći da će objaviti njen HIV status na mreži Facebook).

Ono što je najvažnije, NVO su istakle da trgovci ljudima mogu da koriste IKT, uključujući društvene medije i šifrovane aplikacije, da **nastave kontakt** sa žrtvom trgovine ljudima čak i nakon što je žrtva napustila situaciju eksploatacije – često kako bi je sprečili da podnese pritužbu i traži pravdu. U Holandiji, CKM je utvrdio da je to slučaj kod otprilike jedne trećine žrtava sa kojima su razgovarali (dokazi koje je pružila La Strada International).

### 1.2.4. Trendovi u nastajanju

Organizacije KOK i La Strada Moldova su zabeležile povećanje eksploatacije dece putem **veb kamera i društvenih medija**. Kako navodi La Strada Moldova, počinioci stupaju u kontakt sa decom na društvenim mrežama ili **putem onlajn igrica**, sprijatelje se sa njima ili simuliraju romantičnu vezu. Ponekad se počinioci predstavljaju kao predstavnici agencija za modeling. Od deteta se zatim traži da podeli intimne fotografije koje se zatim koriste za njegovu ucenu. U tom trenutku, počinioci traže od svojih žrtava da izrade i dele seksualno eksplicitniji sadržaj, kao i da učestvuju u izradi i emitovanju seksualnih radnji uživo. U nekim slučajevima, žrtve su pod pritiskom da regrutuju drugu decu ili se sastaju van mreže radi izvođenja seksualnih radnji (KOK je primetio slične obrasce).

Uopšteno govoreći, La Strada International i KOK su ukazali na sve veće ranjivosti nastale **otkrivanjem velike količine ličnih podataka** na društvenim medijima i drugim onlajn platformama, kao i na sve veću otvorenost sa kojom pojedinci mogu da uspostavljaju intimne kontakte sa nepoznatim ljudima na onlajn platformama[6]. Ovo je izraženije među mlađim generacijama. Iako tehnologija može da pruži značajne mogućnosti i prednosti – uključujući obogaćivanje razmene – ona takođe može da pogorša ranjivosti. Na primer, deljenje seksualno eksplicitnih fotografija (seksting) može da predstavlja rizik vezan za trgovinu ljudima, kao i uopšte rizik od ucenjivanja. Iako još uvek nedostaju statistički podaci, istraživanje koje je naručila La Strada Moldova 2020. godine koje je uključivalo reprezentativni uzorak dece uzrasta 9 – 17 godina pruža neke zanimljive uvide u kontekst. Ovaj rad je otkrio da 13% dece u Republici Moldaviji smatra da je deljenje intimnih fotografija na mreži normalno među ljudima koji se vole[7]; 35% je komuniciralo sa nepoznatim ljudima na mreži, a 20% se sastajalo van mreže sa ljudima koje su upoznali na internetu (među njima, 2% je izjavilo da je uznemireno onim što se desilo na tom sastanku).

6 Takođe treba napomenuti da društveni mediji i uopšteno IKT takođe mogu da pomognu organizacijama civilnog društva da identifikuju i uspostave kontakt sa potencijalnim žrtvama trgovine ljudima (o ovoj temi će biti više reči u Poglavlju 3).

7 Samo 1% ispitanika je izričito reklo da je podelilo intimne (seksualno eksplicitne) fotografije i video zapise. Ovaj rezultat, međutim, treba tumačiti oprezno jer je na njega mogao da utiče efekat društvene poželjnosti.

## 1.3. Dodatni dokazi prikupljeni na osnovu analize okruženja

Iako tehnologija može da utiče na trgovinu ljudima tokom svih njenih faza, njena uloga je od posebnog značaja u odnosu na dve faze procesa: regrutovanje i eksploataciju (Latonero 2012; Di Nicola i drugi. 2017, između ostalih).

Tehnologija može da igra ulogu u fazi **regrutovanja** time što olakšava identifikaciju, lociranje i uspostavljanje kontakta sa potencijalnim žrtvama. Glavna promena koju je donela tehnologija je proširenje dometa trgovaca ljudima u potrazi za žrtvama, uz smanjenje „operativnih troškova" identifikacije i kontakta sa potencijalnim žrtvama (Raets i Janssens 2018). Međutim, imajući u vidu da kasnije interakcije licem u lice i dalje igraju ključnu ulogu, trgovci ljudima se i dalje suočavaju sa ograničenjima razmera njihovih operacija. Kako su u igri različiti mehanizmi u zavisnosti od vrste eksploatacije, ključno je razdvojiti regrutovanje u svrhu seksualne eksploatacije od regrutovanja u svrhu radne eksploatacije.[8]

Kada je reč o regrutovanju žrtava za **seksualnu eksploataciju**, tehnologija može da pomogne pri regrutovanju na dva načina:

a. Može da olakša kreiranje i širenje **oglasa za posao na internetu** koji promovišu mogućnosti za rad, najčešće u inostranstvu, u brojnim sektorima u rasponu od administracije, čišćenja ili brige o deci (Evropol 2014) do zabave, modelinga, usluga pratnje i seksualne industrije (SE 2007; UN.GIFT 2008; Di Nicola i drugi 2017).
b. Može da olakša identifikaciju i kontakt sa potencijalnim žrtvama, često ranjivim pojedincima, putem društvenih medija i drugih aplikacija za lični kontakt (videti, na primer, Di Nicola i drugi 2017).

Ovo se može smatrati specifičnom vrstom **vrbovanja na internetu**. Pristup zasnovan na tehnologiji se često primenjuje u modelu regrutovanja „momak". Konkretne veb lokacije i aplikacije („aplikacije") koje se koriste podležu promenama u zavisnosti od onlajn ponašanja i preferencija koje su specifične za određenu državu. Neki izvori su ukazivali na pojavu prakse pribavljanja „kompromitujućih informacija" tokom regrutovanja, a zatim ucenjivanja žrtava kako bi se ostvarila kontrola (praksa slična „seksualnoj iznudi"; Evropol 2020).

Kada je reč o regrutovanju u svrhu **radne eksploatacije**, tehnologija uglavnom pomaže regrutaciji putem širenja oglasa za posao na internetu. Specifični sektori su identifikovani kao posebno ugroženi: veća je verovatnoća da će žene biti regrutovane za poslove u vezi sa ličnom negom, kućnom negom, frizerskim uslugama i čuvanjem dece, dok je veća verovatnoća da će muškarci biti regrutovani za poslove u vezi sa poljoprivredom, građevinarstvom, transportom i preuzimanjem i dostavljanjem humanitarnih torbi (Evropol 2014; Di Nicola i drugi 2017; videti takođe projekat Fine Tune 2011 i SE 2007). Dodatni identifikovani sektori uključuju: ugostiteljstvo, preradu hrane i pakovanje (Fine Tune Project 2011). Oglasi se mogu objavljivati na legitimnim veb lokacijama koje su dostupne širokoj javnosti, na ad hoc veb lokacijama i/ili distribuirati putem društvenih medija.

Iako se čini da određeni izvori naglašavaju fizičku odvojenost između trgovaca ljudima i žrtava postignutu zahvaljujući tehnologiji (OEBS 2020), stvarnost je složenija. Postoje jaki dokazi koji ukazuju na to da upotreba tehnologije više dopunjuje nego što zamenjuje lične interakcije van mreže. Tehnologiju i interakcije licem u lice je najbolje posmatrati kao integrisane. Vrlo je verovatno da stepen uticaja tehnologije zavisi od faktora specifičnih za određene rizične populacije u određenim državama, uključujući: (a) korišćenje interneta i društvenih medija

8 Nema dokaza da se tehnologija koristi u regrutovanju za druge vrste eksploatacije, uključujući i prisilno prosjačenje.

uopšte; (b) korišćenje interneta i društvenih medija prilikom traženja posla; i (c) tehnološke pismenosti određenih rizičnih grupa.

Istraživanja pokazuju da se žrtve najčešće – ali ne uvek – regrutuju u državi porekla, a zatim iskorišćavaju u inostranstvu. Ovaj zaključak je već naveden u izveštaju Saveta Evrope (2007), a naknadni, iako ograničeni, dokazi samo dodatno potkrepljuju ovu ideju. Sve ukazuje na to da će verovatno biti potrebne bilateralne i multilateralne akcije kako bi se stalo na kraj takvim pojavama.

Kada je reč o **fazi eksploatacije**, tehnologija može da igra ulogu u vezi sa seksualnom eksploatacijom. Međutim, u ovom pregledu nema puno dokaza o primetnoj ulozi tehnologije u kontekstu radne eksploatacije (Di Nicola i drugi 2017; Raets i Janssens 2018, između ostalih).

Kada je reč o **seksualnoj eksploataciji**, tehnologija stupa na scenu na dva različita načina:

a. Može da olakša **kontrolu** koju trgovci ljudima vrše nad žrtvama korišćenjem GPS-a ili drugih mobilnih aplikacija, čime se ograničava potreba da trgovci ljudima budu fizički blizu žrtava. Ucena i upotreba kompromitujućih informacija protiv žrtava su takođe pomenuti kao moguće strategije za vršenje kontrole (Raets i Janssens 2018). Na osnovu retkih dokaza, može se zaključiti da je ucenjivanje žrtava primećeno u relativno malom broju slučajeva analiziranih u Holandiji (8,8% slučajeva, bez datuma; izvor: OEBS 2020).
b. Može da olakša **prodaju** seksualnih usluga koje pružaju žrtve trgovine ljudima putem onlajn oglasa usmerenih na krajnje korisnike. Takvi oglasi se često objavljuju na specijalizovanim veb lokacijama ili ad hoc veb lokacijama.

Sve u svemu, uticaj tehnologije na fazu **transporta** se smatra ograničenim, jer žrtve često putuju dobrovoljno i počinju da doživljavaju prinudu tek kada stignu do države odredišta (faza eksploatacije; dokazi agencija za sprovođenje zakona iz Bugarske, Rumunije i Italije izneti u Di Nicola i drugi 2017). Korišćenje tehnologije u ovoj fazi uglavnom se odnosi na mobilne telefone i aplikacije koje se koriste za organizovanje putovanja i koordinaciju vremena i mesta sastanaka, kao i korišćenje interneta za kupovinu karata i organizovanje putovanja. Iako trgovci ljudima mogu da koriste mračnu mrežu za kupovinu falsifikovanih karata, kao i kompromitovanih podataka o kreditnim karticama koje se zatim koriste za kupovinu (lažnih) putnih isprava, detaljna procena više izvora, kako akademskih tako i javno dostupnih dokumenata organa za sprovođenje zakona, sugeriše da je upotreba mračne mreže i dalje veoma ograničena.

# 2. Izazovi tokom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom tehnologije

Ovo poglavlje istražuje izazove koji nastaju kao posledica upotrebe tehnologije u kontekstu trgovine ljudima. U ovom poglavlju se ne bavimo širim izazovima sa kojima se suočavaju države ugovornice a koji nisu direktno povezani sa upotrebom tehnologije. Ovo poglavlje prvo istražuje izazove koji se tiču istrage, a zatim slede izazovi koji se odnose na krivično gonjenje i međunarodnu saradnju na osnovu dokaza koje su dostavile države ugovornice. Onda slede dokazi prikupljeni od NVO, kao i pregled postojeće literature.

## 2.1. Izazovi tokom istrage

Državama ugovornicama je predstavljena lista od sedam potencijalnih izazova tokom istraga koji su identifikovani na osnovu pregleda postojeće baze znanja, kao i ranijih radova koje su pripremili GRETA, Grupa eksperata Saveta Evrope za borbu protiv trgovine ljudima, i Savet Evrope, uključujući i Radionicu iz 2019. godine pod naslovom „Pojačavanje borbe Saveta Evrope protiv trgovine ljudima u digitalnom dobu"[9]. Slika 3. predstavlja **nivo ozbiljnosti** za svaki od sedam izazova[10].

Slika 3. Nivoi ozbiljnosti izazova tokom istraga


Napomena: Raspon rezultata = [0, 100]

Šifrovanje podataka se smatra najvećim izazovom (rezultat 80). Na suprotnom kraju skale nalazi se nedostatak pomoći kompanija iz privatnog sektora, koji se smatra najmanjim izazovom. Svi izazovi, osim pomoći kompanija iz privatnog sektora, imaju rezultat veći od 50, što znači da se njihov ukupni uticaj smatra većim od „malog" problema.

Ovi izazovi se redom razmatraju u sledećim odeljcima: šifrovanje podataka (2.1.1), veliki obim podataka koji se obrađuju (2.1.2), nedostatak tehničke opreme (2.1.3), nedostatak tehničkih znanja među organima za sprovođenje zakona (2.1.4) i brzina tehnoloških promena (2.1.5). Izazovi koji se odnose na pomoć privatnog sektora razmatraju se u odeljku 4. ovog poglavlja,

9 https://www.coe.int/en/web/anti-human-trafficking/-/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age

10 Za svaki izazov, od država ugovornica je zatraženo da procene njegovu ozbiljnost koristeći skalu od tri stepena („obično nije problem", „mali problem" i „veliki problem"). Takve informacije su zatim pretvorene u nivo time što im je dodeljena vrednost od 0, 1 i 2 redom za „nije problem", „mali problem" i „veliki problem". Rezultati su zatim prikazani u rasponu [0, 100].

dok se izazovi koji proizilaze iz zakonodavnih instrumenata razmatraju u poglavlju 5. Treba napomenuti da su neki od izazova isprepleteni, iako se razmatraju odvojeno. Na primer, šifrovanje (i dešifrovanje) podataka zahteva stalna ulaganja u tehnologiju, kao i u razvoj stručnosti osoblja organa za sprovođenje zakona. Od država ugovornica je takođe zatraženo da navedu sve druge izazove sa kojima se suočavaju pored sedam prethodno navedenih. O tim dodatnim izazovima će biti više reči u odeljku 2.1.6 u nastavku.

### 2.1.1. Šifrovanje podataka

Šifrovanje podataka se smatra najvećim izazovom sa kojim se suočavaju nadležni organi kada sprovode istrage o trgovini ljudima posredstvom IKT. Iako se uticaj TOR/mračne mreže ili šifrovanih telefonskih mreža kao što je Encrochat smatra marginalnim, države su ukazivale na izazove koje donose protokoli za šifrovanje koji se koriste u često korišćenim aplikacijama i onlajn uslugama (kao što su WhatsApp i Telegram). Šifrovanje podataka može da „onemogući vraćanje podataka tokom forenzičke istrage" (albanski nadležni organi). Nadležni organi Bosne i Hercegovine tvrde da „sve više istraga vodi do šifrovanog HHD-a, zaključanih telefonskih uređaja, memorijskih kartica i šifrovanih podataka". Prema nadležnim organima Islanda, većina problema sa kojima se policija suočava potiče od „anonimnih i šifrovanih naloga e-pošte i aplikacija, kao što su Proton-mail ili [pribavljanje] informacija o f.ex. pretplatniku". Praćenje i nadzor su takođe ograničeni, ako ne i nemogući – čak i uz zakonski nalog i suprotno drugim vrstama komunikacije. Austrijski nadležni organi su ukazali na nemogućnost da se internet telefonija (VOIP) stavi pod nadzor, dok su francuski nadležni organi istakli „nemogućnost praćenja sistema za trenutnu razmenu poruka (Whatsapp, Messenger, Tik Tok, Wechat, Snapchat)", čime se stvara „velika prepreka za istrage (poteškoće u identifikaciji počinilaca i žrtava, u uspostavljanju veza među pojedincima i u prikupljanju dokaza o prinudi i podređenosti)"[11]. Belgijski nadležni organi su dalje primetili da istražne aktivnosti koje se sprovode u zatvorenim šifrovanim kanalima zahtevaju korišćenje doušnika i tajnih agenata – a to može da bude problematično u određenim državama (uključujući Belgiju). Nadležni organi u Irskoj su izrazili stav da „šifrovanje postaje sve jače" – što je ponovilo i nekoliko drugih država ugovornica. Raznovrsnost šifrovanih tehnologija dostupnih široj javnosti raste, sa sve više aplikacija za trenutnu razmenu poruka koje su dizajnirane da maksimalno pojačaju šifrovanje i maksimalno smanje količinu generisanih korisničkih podataka (npr. Threema ili Signal).

Kao što je navedeno u prijavi koju je podnela Švajcarska, uticaj šifrovanja varira u zavisnosti od toga da li istražitelji imaju pristup fizičkom uređaju ili ne. Ako je uređaj fizički u rukama istražitelja, onda je „šifrovanje podataka manji problem, a podatke mogu da dešifruju specijalizovane policijske službe" (slično navodi i Luksemburg). Međutim, policajci sa ovim tehničkim veštinama su malobrojni i ove službe će verovatno biti preopterećene – što dovodi do odlaganja istraga. Ako agencije za sprovođenje zakona nemaju pristup fizičkoj podršci, onda su „istrage otežane" (prijava koju je podnela Švajcarska). U nekim državama, na primer u Ujedinjenom Kraljevstvu, policijske snage imaju ovlašćenje da od osobe zahtevaju da preda lozinku ili PIN za svoj mobilni telefon. Međutim, kako se ističe u dokazima koje su dostavili britanski organi, problemi i dalje ostaju: „čak i nakon hapšenja i zaplene takvih uređaja, mogu da se jave prepreke za pristup važnim komunikacijama", naročito kod uređaja sa visokim nivoom bezbednosnih funkcija. Ovo su ponovili i belgijski nadležni organi, koji su ukazali na poteškoće u dešifrovanju najsofisticiranijih algoritama (zato su pozvali na više ulaganja u nove alate za dešifrovanje).

Nekoliko država je nagovestilo postojanje alata za dešifrovanje bar nekih vrsta algoritama. Jasno je, međutim, da je ovo okruženje koje se neprekidno razvija i zahteva (velika) ulaganja,

11 Ovo je takođe primećeno u dokazima koje su dostavili grčki nadležni organi.

kako u obuke, tako i u softver. Koraci preduzeti za prevazilaženje ovog problema uključuju uspostavljanje jedinica/centara za borbu protiv sajber-kriminala čiji zadatak je rad sa tehnologijom za dešifrovanje. To je slučaj, na primer, sa Norveškom. Slično tome, Francuska trenutno radi na razvoju uređaja za razbijanje lozinki „na centralnom nivou".

Slovenački nadležni organi su otvorili pitanje troškova vezanih za dešifrovanje elektronskih podataka. Takvi troškovi nastaju kao posledica potrebe za angažovanjem specijalizovanog, visoko obučenog osoblja, kao i kupovine specijalizovanih delova softvera koji mogu da zaobiđu šifrovanje. Štaviše, kako se protokoli za šifrovanje neprestano razvijaju, postoji potreba da se softver stalno ažurira, što je često praćeno ogromnim naknadama za licencu.

Osim toga, moglo bi biti korisno da se resursi udruže na nadnacionalnom nivou za potrebe razvoja tehnoloških proizvoda, kao što su softver za dešifrovanje i skeniranje mreže radi prikupljanja podataka, kako su, na primer, predložili nadležni organi iz Švedske. Sve u svemu, iz dostavljenih dokaza proizilazi da se više može učiniti u pogledu **podsticanja razmene znanja i udruživanja radi zajedničkog razvoja tehnologije** u različitim državama. Bliža i adekvatno finansirana tehnička saradnja se pokazala veoma uspešnom, na primer u infiltraciji u šifrovanu mrežu za razmenu poruka Encrochat koju koriste organizovane kriminalne grupe na visokom nivou širom Evrope (ovo je dovelo do više istraga i suđenja visokog profila u Francuskoj, Holandiji, Ujedinjenom Kraljevstvu i Švedskoj, između ostalih država).

U nekim slučajevima, kako su istakli francuski nadležni organi, šifrovanje se može prevazići korišćenjem alternativnih istražnih tehnika, na primer korišćenjem „tehničkog nadzora telefonskih linija žrtava [koji] ostaje efikasno sredstvo dok se čeka tehnologija koja će omogućiti da se zaobiđe šifrovanje".

### 2.1.2. Velike količine podataka

Elektronske komunikacije i IKT uređaji generišu sve veću količinu podataka, što zauzvrat može da predstavlja ogroman napor za istražitelje. Kako je istaklo nekoliko država, velika količina generisanih podataka utiče na mogućnost njihovog izdvajanja, što zahteva moćnu tehničku opremu. Jednako izazovna je analiza i pažljivo ispitivanje velikih količina informacija. Pametni telefoni imaju sve veći kapacitet memorije; dokazi koje generišu korisnici mogu biti dostupni u više oblika: (dugačka) ćaskanja, ali i fotografije, snimci i glasovne poruke za čiju su analizu potrebne „nedelje" (dokazi iz Švajcarske). Ovaj izazov je posebno naglašen u slučajevima kada „ne može da se izvrši pretraga po specifičnim ključnim rečima i [istražitelji] moraju da pregledaju sve podatke" (dokazi iz Švajcarske). Prema švajcarskim nadležnim organima, „iskustvo i praksa su pokazali da se količina podataka značajno povećala sa modernim društvenim medijima, što potencijalno dovodi do veoma dugih istražnih aktivnosti [...] koje mogu da drže istražitelja zauzetim mesecima i da dovedu do uskih grla u resursima".

Velika količina podataka često zahteva specijalizovane delove softvera, kao i posebnu obuku o tome kako da se podaci sistematizuju i pretražuju u okviru tako velikog broja dokaza. Prema britanskim nadležnim organima, „internet tržišta i društvene mreže generišu ogromnu količinu podataka [koju] može biti teško raščlaniti, a skupo je licencirati ili razvijati alate koji mogu efikasno da analiziraju ove podatke". Francuski nadležni organi su podjednako naglasili potrebu za razvojem alata koji bi mogli da pomognu istražiteljima u rukovanju velikim količinama podataka, na primer pomoću algoritama veštačke inteligencije (AI) (slično su istakli i nadležni organi Španije). Prema norveškim nadležnim organima, količina elektronskih podataka čini

„istrage složenijim, sa potrebom za korišćenjem istražnih metoda zasnovanih na tehnologiji"[12]. Takve metode, međutim, često „dovode do velike količine podataka [od kojih] je samo mali deo [...] koristan za istragu".

Postoji opšta saglasnost da je razvoj kapaciteta za rukovanje velikim količinama elektronskih dokaza od ključnog značaja. Međutim, takav kapacitet treba stalno da se ažurira kako bi se držao korak sa „internet omogućivačima koji se stalno menjaju zbog brzine tehnoloških promena" (prijava britanskih nadležnih organa). Ovo ponavljaju i holandski nadležni organi, koji su ukazali na sve veću količinu podataka koje generišu onlajn platforme i društveni mediji, kao i na izazov koji donosi **promena obrazaca ponašanja** njihovih korisnika, zbog čega je „teško otkriti gde treba tražiti". Dostupnost digitalnih alata smatra se prvim (neophodnim) korakom; međutim, stalno prilagođavanje tehnološkom i bihevioralnoj digitalnoj sredini predstavlja izazovan, ali neophodan sledeći korak.

Ono što dodatno pogoršava problem je to što velike količine podataka često treba da se obrađuju i analiziraju u kratkom roku. Na primer, kada se osumnjičeni privede, službenici su pod vremenskim pritiskom da vrlo brzo pregledaju veliku količinu elektronskih dokaza – kako ističu slovenački nadležni organi. Ograničeno vreme koje je često istražiteljima na raspolaganju da pregledaju materijal zahteva „**bolju tehnologiju za pretragu i sortiranje informacija**" (dokazi iz Ujedinjenog Kraljevstva). Štaviše, nekoliko država ugovornica je istaklo da su elektronski podaci prikupljeni u kontekstu istraga trgovine ljudima često na jeziku koji istražitelji najčešće ne govore, što zahteva duge i skupe prevode (ovo pitanje je posebno akutno među državama odredišta).

### 2.1.3. Nedostatak tehničke opreme

Nekoliko država je istaklo nedostatak tehničke opreme kao veliki izazov za sprovođenje istraga. Ovo uključuje često nedovoljan broj mašina koje mogu da izvršavaju specijalizovane zadatke, kao što je razbijanje šifri, kao i poteškoće u praćenju razvoja softvera i hardvera. Kao što je već pomenuto, specijalizovani softveri i hardveri mogu da budu skupi i često zahtevaju stalna ažuriranja i skupe ugovore o licenciranju kako bi pratili korak sa brzinom tehnoloških promena. Ovo može da ima značajan uticaj na budžet policije. Države sa manjom kupovnom moći teško ispunjavaju zahteve u pogledu tehničke opremljenosti. Da nije bilo podrške međunarodnih partnera i donatora iz privatnog sektora, neke države bi već bile izgurane sa međunarodnog tržišta specijalizovanih tehničkih alata (ovo izričito navode nadležni organi iz Albanije, ali takođe proizilazi iz prijava drugih država). Međutim, ovo nipošto nije pitanje ograničeno na države sa manje raspoloživih resursa. Nemačka, Belgija, Švedska, Francuska i Ujedinjeno Kraljevstvo, između ostalih, izrazili su ozbiljnu zabrinutost zbog cene specijalizovanog softvera i hardverske opreme.

Većina slučajeva trgovine ljudima je međunarodne prirode i često uključuje žrtve iz manje bogatih država koje se eksploatišu u bogatijim državama. Ovo u konkretnim slučajevima stvara potrebu za međunarodnom saradnjom među državama. To se takođe pretvara u često zanemarenu potrebu za ojačanim programima tehnološke pomoći koje podržavaju države odredišta u korist država izvora (tj. država porekla žrtava) – pored postojećih multilateralnih programa, poput onih koje vodi Evropska unija a koji već pružaju finansijsku podršku za nadogradnju tehnološke opreme.

12 Nadležni organi iz Portugala su izneli isto opažanje.

### 2.1.4. Nedostatak tehničkog znanja među organima za sprovođenje zakona

Upotrebljivost same tehničke opreme je ograničena ako nema adekvatnih obuka koje su dostupne agencijama za sprovođenje zakona. Uopšteno govoreći, ulaganja u ljudski kapital, odnosno u obuke i tehničko znanje policijskih službenika, jednako su važna kao i ulaganja u softver i hardver – ako ne i važnija. Države ugovornice često pominju potrebu da se obezbede takve obuke i dodatna tehnička znanja za policijske službenike. Prema rečima nadležnih organa u Belgiji, „imperativ" je da se smanji „**digitalna podela između počinilaca i policijskih snaga**". Države ugovornice su identifikovale različite potrebe za znanjem.

Prvo, postoji potreba za razvojem znanja o pojavi novih trendova i promenama u korišćenju tehnologije od strane počinilaca i žrtava. Drugo, države su istakle značaj razvoja znanja o pojavi novih aplikacija i usluga na tehnološkom tržištu koje karakterišu brze promene. Treće, postoji potreba da se prati korak sa razvojem novih bezbednosnih protokola i metoda šifrovanja. Ono što je najvažnije, znanje treba mudro rasporediti unutar organizacije. Na primer, nedostatak specijalizovanih službenika na lokalnom nivou može da stvori **uska grla u istragama**, ako je potrebno više puta tražiti pomoć od (preopterećene) centralizovane jedinice. Ovo je ključno pitanje na koje države treba da obrate odgovarajuću pažnju – i to je dokazano u prijavama nekoliko država ugovornica, uključujući Albaniju, Belgiju, Island, Francusku, Portugal, Slovačku i Sloveniju (videti Poglavlje 4 za detaljnije diskusije o obukama).

Nekoliko država je istaklo potrebu za **organizovanjem dodatnih tehničkih obuka za „opšte" policijske službenike**. Pored obuka za specijalizovane službenike sa bogatim tehničkim znanjem u vezi sa specifičnim delovima softvera ili tehnikama dešifrovanja, postoji potreba da se svim službenicima obezbedi osnovni skup digitalnih veština i tehničkih znanja. Ključno je da službenici koji prvi izlaze na mesto zločina poseduju takva znanja. Kako su primetili albanski nadležni organi, greške koje naprave osobe koje prve izlaze na mesto zločina „mogu biti fatalne kada je reč o prikupljanju elektronskih dokaza, [koji] onda postaju nevažeći za dalju analizu". Za najveći broj službenika potrebno je organizovati odgovarajuću obuku o prikupljanju i rukovanju **elektronskim dokazima**. Štaviše, razvoj stručnosti u ovoj oblasti treba da bude redovna tema u nastavnim planovima i programima obuka za policijske službenike.

Pored toga, iako bi osnovni nivo tehničkog znanja bio prava prednost za sve istražitelje, mogu se desiti složeniji slučajevi u kojima će možda biti potrebno formirati timove sa multidisciplinarnim skupovima veština (npr. okupljanjem istražitelja, stručnjaka za finansijski i visokotehnološki kriminal). Države bi možda želele da razmotre uvođenje – ili unapređenje – odredbi koje omogućavaju brzo formiranje takvih timova, kad god je to potrebno, ili čak da interdisciplinarni timovi postanu sastavni deo savremenog policijskog rada. Ovo bi se moglo proširiti na međunarodne zajedničke istražne timove, npr. uključivanjem stručnjaka za tehnologiju i komunikacije u takve timove (što su istakli bugarski nadležni organi).

Švajcarski nadležni organi primećuju da je „držanje koraka sa tehnološkim napretkom veliki izazov za organe za sprovođenje zakona", a današnjim istražiteljima je potrebna ekspertiza i za trgovinu ljudima i za IKT, uključujući korišćenje društvenih medija i tehničke veštine. Francuski nadležni organi su izrazili potrebu da obuče više osoblja za korišćenje novih tehnologija, kao i za finansijske istrage. Nadležni organi Bugarske su izvestili o primeru u kojem je u saradnji sa francuskim nadležnim organima korišćena kombinacija istražnih tehnika na mreži i van mreže. Polazeći od otkrića pornografskih slika dece, istražitelji su uspeli da prvo

identifikuju IP adresu, a zatim da je fizički lociraju u hotelu. Kada su upali u hotel, pronašli su brojne žene koje su bile prisiljene da pružaju seksualne usluge i došli do niza Facebook pseudonima drugih žrtava, koje su potom identifikovane pomoću njihovih Facebook profila. Na kraju je identifikovano 60 žrtava trgovine ljudima u svrhu seksualne eksploatacije, jedno dete žrtva koje je bilo prinuđeno da proizvodi pornografski materijal, kao i 18 počinilaca. Ovaj slučaj ukazuje na potrebu da istražitelji budu dobro upućeni u onlajn i oflajn istražne tehnike, jer je sve veća verovatnoća da će obe tehnike morati da se koriste tokom istraga trgovine ljudima. To bi, naravno, zahtevalo kontinuiranu obuku.

### 2.1.5. Brzina tehnoloških promena

Brzi tempo tehnoloških promena je sveobuhvatno pitanje koje utiče na sve gore navedene izazove: šifrovanje, obuku policajaca, tehnološku opremu i prikupljanje elektronskih dokaza. Molimo pogledajte diskusiju iznad za više detalja.

### 2.1.6. Dodatni izazovi tokom istraga

Brojne države su označile problem u vezi sa (neadekvatnim) **obavezama čuvanja podataka** koje su nametnute pružaocima internet usluga (ISP) i u vezi sa njihovim uticajem na istrage. U Bugarskoj, na primer, postojeće zakonodavstvo zahteva od ISP da čuvaju takve podatke šest meseci – trajanje koje se smatra neadekvatnim za razvoj jakih istraga. Dužinu čuvanja podataka takođe su naveli nadležni organi Holandije i Malte. Norveški nadležni organi su napomenuli da, prema nacionalnom zakonodavstvu, ISP-ovima nije dozvoljeno da čuvaju informacije o IP adresama duže od 21 dan i od njih se ne traži da čuvaju podatke o vezi između pretplatnika i IP adrese. Bugarski i rumunski nadležni organi pozvali su na usaglašavanje nacionalnih propisa koji uređuju čuvanje podataka o internet saobraćaju, kao i istražnih praksi u vezi sa prekršajima posredstvom IKT-a.

Zabrana trojanaca (tj. špijunskog softvera) smatra se dodatnim izazovom za istrage uz pomoć IKT, jer agencijama za sprovođenje zakona nije dozvoljeno da uđu u domove i druge prostorije da instaliraju špijunski softver na uređaje koje koriste pojedinci koji su predmet istrage. Nadležni organi tvrde da bi takvi alati omogućili agencijama za sprovođenje zakona da ublaže probleme u vezi sa šifrovanjem, kao i poteškoće u prisluškivanju VOIP razgovora. Belgijski nadležni organi pozvali su na izmene pravnog okvira kako bi se olakšao istražni rad pomoću novih tehnologija. Oni su istakli potrebu za pojednostavljenjem procedura i pravnih sredstava uzimajući u obzir *modus operandi* počinilaca.

Bugarski nadležni organi su pokrenuli pitanje u vezi sa elektronskim dokazima, posebno ističući potrebu da se uvedu međunarodni zahtevi koji bi od ISP tražili da implementiraju odgovarajuće bezbednosne protokole koji sprečavaju bilo kakvo **neovlašćeno menjanje podataka,** kako tokom čuvanja, tako i tokom prenosa organima za sprovođenje zakona.

Holandski nadležni organi su pokrenuli pitanje vezano za primenu **zakona o privatnosti**, na primer u kontekstu korišćenja sistema za skeniranje mreže radi prikupljanja podataka.

Nadležni organi u Španiji su zatražili da veći broj zaposlenih bude specijalizovan za borbu protiv trgovine ljudima i napredne veštine korišćenja računara. Nadležni organi iz Belgije su izneli isto opažanje.

Moldavski nadležni organi su ukazali na poteškoće u zadržavanju kvalifikovanih praktičara jer službenici sa iskustvom često napuštaju specijalizovane jedinice kako bi se pridružili drugim sektorima pravosuđa ili privatnom sektoru, i naglasili su značaj redovnih provera motivacije za privlačenje i zadržavanje talenata.

Austrijski nadležni organi su istakli problem sa kaznama koje su predviđene za trgovinu ljudima u njihovom nacionalnom Krivičnom zakoniku, a koje predviđaju kaznu zatvora između šest meseci i 10 godina. Iako je ova kazna dovoljna za praćenje poruka po nalogu suda, ona ne daje policijskim snagama pravo da koriste vizuelni i akustični nadzor (tj. audio nadzor privatnih razgovora i privatnih prostorija).

Britanski nadležni organi su primetili izazove kada je reč o IP adresama i elektronskim dokazima. IP adrese su početna tačka u istrazi i, kada se pribave, organi za sprovođenje zakona moraju da upare te IP adrese sa različitim korisničkim imenima i korisnicima. Međutim, korisnička imena se mogu promeniti u bilo kom trenutku i osumnjičeni ih često koriste naizmenično. Od ključnog je značaja da organi za sprovođenje zakona proveravaju kontinuitet IP adresa u odnosu na korisnička imena. Pored toga, u virtuelnim sobama za ćaskanje, neki korisnici se mogu videti na ekranu – i njihov identitet je dokazan – ali možda ima i drugih koji nemaju uključene veb kamere. Neki osumnjičeni mogu da dele uređaje sa drugima, na primer ako se nalaze u domaćinstvu sa više stanara, što zauzvrat može da oteža njihovu identifikaciju.

Britanski nadležni organi su takođe pokrenuli pitanje postupanja sa neiskorišćenim elektronskim materijalom, posebno u kontekstu obaveza po osnovu GDPR. U istom smislu, holandski nadležni organi smatraju da međunarodni propisi o zaštiti podataka „ometaju prikupljanje, čuvanje i obradu informacija pribavljenih tehnološkim istražnim tehnikama (kao što su sistemi za skeniranje mreže radi prikupljanja podataka)", čime „sprečavaju optimalnu upotrebu [takvih] tehnika".

## ZOOM | Izazovi u otkrivanju slučajeva trgovine ljudima posredstvom IKT

Istrage i krivično gonjenje zavise od otkrivanja slučajeva. U nastavku su navedeni izazovi koje su identifikovale države kada je reč o otkrivanju trgovine ljudima posredstvom IKT:

- Internet predstavlja veoma velik prostor za praćenje, a obim onlajn aktivnosti/interakcija neprekidno raste. Onlajn resursi obuhvataju veoma širok i raznolik spektar, od stranica za oglašavanje na mreži i veb lokacija za odrasle, do platformi društvenih medija, soba za ćaskanje i potencijalno mračne mreže. Nadzor nad takvim prostorom zahteva ogromne resurse i podleže zakonskim ograničenjima (zakoni o privatnosti i ograničenja korišćenja sistema za skeniranje mreže radi prikupljanja podataka u nekim državama).
- Ručno pretraživanje veb lokacija na internetu je izuzetno izazovno, dok velike količine nestrukturisanih podataka otežavaju skeniranje mreže radi prikupljanja podataka (ako je to uopšte dozvoljeno nacionalnim zakonodavstvom). Broj onlajn oglasa (otvorenih i malih oglasa) za seksualne i neseksualne usluge često je prevelik za ručno pretraživanje.
- Poteškoće prilikom identifikacije počinilaca i žrtava, jer mogu da koriste nadimke i pseudonime tokom svojih onlajn aktivnosti. Softver za anonimizaciju (npr. VPN) i upotreba šifrovane komunikacije između trgovaca ljudima i žrtava dodatno otežavaju identifikaciju. Razgovori između trgovaca ljudima i žrtava odvijaju se u zatvorenim grupama (npr. Facebook, WhatsApp, Telegram).
- Ponašanje korisnika interneta koje se brzo menja (npr. nova tehnologija se pojavljuje, nove veb lokacije/aplikacije postaju popularne za kratko vreme). Pored toga, brzo se pojavljuju novi alati, podstaknuti jakom konkurencijom u tehnološkom sektoru, koji trgovcima ljudima mogu da pruže nova sredstva za povezivanje i eksploataciju žrtava.
- Izazovi prilikom sortiranja onlajn oglasa kako bi se identifikovali oni koji se odnose na trgovinu ljudima u kontekstu seksualnih i neseksualnih usluga. Oglasi za seksualne usluge koje objavljuju žrtve trgovine ljudima često koriste iste stranice, istu terminologiju i iste formulacije kao oni koje objavljuju nezavisni seksualni radnici. „Znaci upozorenja" za identifikaciju oglasa povezanih sa radnom eksploatacijom su još uvek nedovoljno razvijeni ili se ne koriste dosledno.
- Odsustvo specijalizovanih jedinica u policiji i/ili nedostatak specijalizovanih istražitelja za slučajeva trgovine ljudima sa naprednim veštinama korišćenja računara. Nedostatak službenika obučenih za izvođenje tajnih operacija na internetu (npr. stvaranjem i održavanjem „lažnog" profila).
- Nedostatak obuka za policijske službenike o specifičnostima trgovine ljudima posredstvom IKT (npr. *modus operandi* počinilaca, platforme na kojima se trgovina odvija, kako tajno pristupiti trgovcima ljudima i kreirati kredibilne profile na internetu).
- Mogućnost uklanjanja/menjanja razgovora (elektronskih dokaza) od strane trgovaca ljudima.
- Proces slanja zahteva kompanijama koje upravljaju društvenim medijima (često sa sedištem u stranoj državi) koji oduzima mnogo vremena i nedostatak reakcije nekih kompanija.
- Kratki periodi čuvanja IP adresa i poteškoće oko pristupanja takvim podacima.
- Jezičke barijere.

## 2.2. Izazovi tokom krivičnog gonjenja

Državama ugovornicama je predstavljena lista od šest potencijalnih izazova tokom krivičnog gonjenja, a koji su identifikovani na osnovu pregleda trenutne baze znanja, kao i ranijih radova koje je pripremio Savet Evrope, uključujući i Radionicu iz 2019. godine pod naslovom „Pojačavanje borbe Saveta Evrope protiv trgovine ljudima u digitalnom dobu"[13]. Slika 4. predstavlja **nivo ozbiljnosti** za svaki od šest izazova[14].

Slika 4. Nivoi ozbiljnosti izazova tokom krivičnog gonjenja


Napomena: Raspon rezultata = [0, 100]

Sve u svemu, izazovi tokom krivičnog gonjenja imaju niže ocene od onih tokom istrage, pri čemu je samo za „pribavljanje dokaza iz drugih država" ocena nešto viša od 50 (ocene veće od 50 ukazuju na to da se izazov često doživljava kao ozbiljniji od samo „manjeg problema"). Ovo je verovatno zbog činjenice da, ako je slučaj zaista stigao u fazu krivičnog gonjenja, većina prepreka je uspešno otklonjena tokom faze istrage.

U nastavku navodimo još neke kvalitativne dokaze o tri izazova: utvrđivanje nadležnosti, ekstradicija osumnjičenih i obuka tužilaca. Izazovi koji se odnose na pomoć privatnog sektora razmatraju se u odeljku 2.4, dok su izazovi koji proizilaze iz zakonodavnih instrumenata razmatrani u poglavlju 5. Izazovi u vezi sa pribavljanjem dokaza iz drugih država razmatrani su u odeljku 2.3, i predstavljaju prepreke međunarodnoj saradnji.

- *Utvrđivanje nadležnosti*: Dok se generalno smatra da je utvrđivanje nadležnosti manji izazov među državama ugovornicama, povremeni problemi mogu da se pojave u slučajevima koji su omogućeni IKT-om a tiču se istovremenih nadležnosti. U nekim slučajevima mogu se pojaviti izazovi pri identifikaciji osumnjičenih i, što je najvažnije, pri utvrđivanju njihove lokacije, što znači povezivanje određene IP adrese sa određenom osobom, a zatim te osobe sa lokacijom u određenoj državi.
- *Ekstradicija osumnjičenih*: Sve u svemu, ovo se posmatra kao relativno mali problem. Evropski nalog za hapšenje (EAW) i Evropski nalog za istragu (EIO) su dva važna alata

13 https://www.coe.int/en/web/anti-human-trafficking/-/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age

14 Za svaki izazov, od država ugovornica je zatraženo da procene njegovu ozbiljnost koristeći skalu od tri stepena („obično nije problem", „mali problem" i „veliki problem"). Takve informacije su zatim pretvorene u nivo time što im je dodeljena vrednost od 0, 1 i 2 za „nije problem", „mali problem" i „veliki problem". Rezultati su zatim prikazani u rasponu [0, 100].

koji su „omogućili da se efikasno (i takođe određenom brzinom) odgovori na izazove koje predstavlja transnacionalnost" (portugalski nadležni organi). Kao primer dobre prakse pominje se rad Evrodžasta. Nadležni organi Švajcarske su ukazali na prepreke sa kojima se suočavaju jer nisu u mogućnosti da izdaju evropski nalog za hapšenje i evropski nalog za istragu. Slično tome, britanski nadležni organi su naveli da „izlazak Ujedinjenog Kraljevstva iz EU može da utiče na ekstradiciju" jer „zabrana državljanstva nekih država znači da [Ujedinjeno Kraljevstvo] više ne može da izruči neke državljane EU i zahteva diskusiju o tome koja država vrši krivično gonjenje". Razlike u zakonima o trgovini ljudima između država mogu da stvore izazove u pogledu ekstradicije osumnjičenih.

- *Obuka tužilaca*: Nekoliko država je istaklo značaj odgovarajuće obuke za tužioce o trgovini ljudima posredstvom IKT, napominjući da u nekim slučajevima ova obuka nedostaje ili nije adekvatna. Obuka tužilaca se smatra ključnom kako bi se osiguralo da predmeti koji se razvijaju uz pomoć IKT-a budu robusni, da se elektronski dokazi pravilno prikupljaju i koriste i da se predmeti (i dokazi u njima) na odgovarajući način izvode pred sudijom/porotom. Neke države, poput Norveške, planiraju da pojačaju takvu obuku tako što će dovesti tužioca sa iskustvom u predmetima trgovine ljudima koji će držati predavanja kolegama. Osim toga, stručnost možda neće biti stalno dostupna u svim tužilaštvima u državi. Ovaj problem su, između ostalih, primetili i holandski nadležni organi. Kao odgovor, holandsko tužilaštvo, zajedno sa nacionalnom policijom, trenutno procenjuje nivo stručnosti u ovoj službi. Takav proces unutar državnog praćenja može se smatrati primerom dobre prakse kako bi se obezbedila doslednost u nivou stručnosti u okviru države. Osim toga, neke države ugovornice su zabeležile slučajeve u kojima tužioci nisu bili upoznati sa procedurom traženja elektronskih podataka od privatnih kompanija; u drugim slučajevima, tužioci nisu bili upoznati sa procedurama za pribavljanje dokaza od drugih država i traženje njihove saradnje, na primer uspostavljanjem zajedničkog istražnog tima ili izdavanjem evropskog naloga za istragu. Unapređena obuka za tužioce bi trebalo da olakša proces povezivanja sa drugim državama, kao i privatnim kompanijama. Na kraju, države ugovornice su izrazile stav da interdisciplinarnu obuku sa elementima trgovine ljudima i IKT treba proširiti na sudije.

Osim toga, od država ugovornica je zatraženo da navedu sve **dodatne izazove** sa kojima se suočavaju u procesuiranju slučajeva trgovine ljudima posredstvom IKT. U nastavku je dat pregled identifikovanih izazova:

- Britanski nadležni organi su označili problem u dokazivanju učešća i *mens rea* pojedinačnih počinilaca u slučajevima koji su omogućeni IKT-om kada postoji grupna aktivnost, na primer u internet sobi za ćaskanje gde jedan ekran možda prikazuje zlostavljanje žrtve trgovine ljudima, dok drugi ekrani možda prikazuju druge korisnike koji učestvuju u aktivnostima odraslih koje se obavljaju uz njihovu saglasnost. Dokazivanje učešća različitih pojedinaca može da predstavlja izazov s obzirom na različite uloge.
- Još jedan izazov koji su britanski nadležni organi istakli u prijavi odnosi se na izvođenje dokaza pred porotom (ili sudijom). U slučajevima do kojih dolazi posredstvom IKT, izvođenje tehničkih dokaza često radi stručnjak koji je upoznat sa tehnologijom (koji objašnjava kako, na primer, funkcioniše emitovanje uživo iz internet soba za ćaskanje, koje su njegove funkcije i koji snimci su možda snimljeni, uključujući opis šta kakav snimak prikazuje).

Razvijanje interne stručnosti među službenicima o tome kako efikasno i tačno izvesti elektronske dokaze sve više dobija na značaju. Srodan izazov odnosi se na izvođenje velikih količina elektronskog materijala pred porotom. Rešenje koje se razmatra u Ujedinjenom Kraljevstvu je upotreba tableta.

## 2.3. Izazovi međunarodne saradnje

Tokom studije je od država ugovornica traženo da ukažu na izazove sa kojima se suočavaju u vezi sa transnacionalnim istragama i pravosudnom saradnjom u kontekstu trgovine ljudima posredstvom IKT. Većina navedenih izazova nije specifična za trgovinu ljudima posredstvom IKT, ali uopšteno utiče na prekogranične istrage i pravosudnu saradnju, na primer, jezičke barijere, različiti pravni osnovi, koordinacija paralelnih istraga, brza razmena informacija. Međutim, specifičnosti trgovine ljudima posredstvom IKT često ih pogoršavaju. Ovo je posebno akutno u slučaju elektronskih dokaza. Pored toga, u kontekstu trgovine ljudima posredstvom IKT, primanje uzajamne pravne pomoći i obezbeđivanje dokaza često imaju kritičnu vremensku komponentu.

### 2.3.1. Zahtevi za uzajamnu pravnu pomoć

Većina država ugovornica je označila dugo vreme potrebno za obradu zahteva za uzajamnu pravnu pomoć (UPP) kao jednu od glavnih prepreka međunarodnoj saradnji. Sve u svemu, postupci traženja uzajamne pravne pomoći smatraju se sporim, ponekad nepredvidivim i takvim da su im potrebni međunarodno dogovoreni jedinstveni obrasci. Kako su primetili španski nadležni organi, „ima previše izvora informacija koji zahtevaju sudsko odobrenje kako bi im se pristupilo". Takvi zahtevi moraju da budu obrađeni putem uzajamne pravne pomoći, što zauzvrat komplikuje i produžava tok istrage. Postojeći sistem je nekoliko država okarakterisalo kao „neadekvatan". Zahtevi za uzajamnu pravnu pomoć između država ugovornica SE mogu se odvijati u okviru dva različita scenarija: (a) u okviru pravosudne saradnje EU (uključujući pomoć Evropola i džasta) i (b) van okvira EU. Kako izazovi i procedure mogu biti drastično različiti u zavisnosti od scenarija, važno je da se razmotre odvojeno.

*Saradnja u okviru pravnog okvira EU*. Države ugovornice Saveta Evrope koje su takođe države članice Evropske unije vide koordinisani okvir policijske i pravosudne saradnje na nivou EU kao koristan i sposoban da ujednači proces. To uključuje rad agencija EU kao što su Evrodžast i Evropol. Međutim, izazovi i dalje postoje. Prema francuskim nadležnim organima, „instrumenti međunarodne saradnje, iako zanimljivi, su ipak spori: za evropski nalog za istragu (EIO) potrebno je nekoliko meseci, a zajednički istražni tim (ZIT) je teško sprovesti". Jedna od glavnih prepreka sprovođenju zajedničkih istražnih timova je potreba za identičnom istragom u drugoj državi ili u više njih. Na ovo su takođe ukazali nadležni organi Norveške.

*Saradnja izvan pravnog okvira EU*. Ovo se posmatra kao proces koji oduzima više vremena i karakteriše ga veća zamršenost nego u scenariju navedenom iznad zbog nedostatka usaglašenosti između različitih pravnih sistema (kao što su istakli, između ostalog, kiparski i španski nadležni organi). Švajcarski nadležni organi su primetili da odgovor na „zahteve za međunarodnu pravnu pomoć često zavisi od dobre volje ili interesa stranih tužilaca". Ovo unosi element nepredvidljivosti i nedoslednosti u proces. Takvi „pregovori između tužilaštava su često dugotrajni". **Jasnije operativne procedure, poboljšana redovna razmena između kontaktnih tačaka i zahtevi za UPP, jasno postavljeni** i razmotreni na samom početku, doprineli bi usaglašavanju procesa. Nadležni organi u Severnoj Makedoniji primetili su da svi zahtevi za uzajamnu pravnu pomoć moraju da prođu kroz centralizovanu jedinicu u okviru Ministarstva pravde, što stvara usko grlo i često usporava procedure. Predložili su da se osmisle alternativni mehanizmi koji bi omogućili određenim ključnim institucijama da uspostave direktan kontakt sa svojim međunarodnim kolegama (npr. javno tužilaštvo, inspektorat rada, ministarstvo unutrašnjih poslova).

Norveški nadležni organi su ukazali na potrebu da se unaprede postojeći sporazumi i da se uspostave novi sporazumi sa državama porekla žrtava kada su one van EU. Ovo je pitanje koje su pokrenuli i francuski nadležni organi, koje su naglasili da „određeni broj kriminalnih organizacija koje koriste IKT potiče iz država sa kojima je međunarodna saradnja ili nedovoljna ili nepostojeća. To je slučaj sa kineskim mrežama i mrežama iz Rusije i Ukrajine". Zahvaljujući IKT, ove kriminalne mreže mogu da organizuju svoje operacije na način koji omogućava glavnim članovima da kontrolišu aktivnosti prostitucije iz svoje države porekla – često znajući da zahtevi za pravosudnu saradnju neće biti blagovremeno ispunjeni, ako uopšte budu ispunjeni. Spora saradnja ili odsustvo saradnje utiču na identifikaciju počinilaca, prikupljanje dokaza i gašenje veb lokacija.

### ZOOM | Šta se može naučiti iz pravosudnog okvira EU?

Nema sumnje da pravosudni okvir EU nudi integrisaniji pravni prostor koji može da olakša pravosudnu saradnju u poređenju sa situacijom sa kojom se države ugovornice suočavaju kada traže saradnju izvan takvog okvira (iako sa ograničenjima i izazovima). Koji elementi takvog okvira bi se mogli proširiti izvan saradnje unutar EU? Ovo je teško pitanje koje zahteva sveobuhvatnu pravnu analizu, ali ovde možemo ukratko navesti neke preliminarne sugestije. Prijava nadležnih organa iz Švajcarske (tj. države izvan pravosudnog okvira EU) lepo sumira ključne prednosti okvira EU, a naročito Evropskog naloga za istragu (EIO):

- zasniva se na zajedničkom skupu pravila sa širokom oblašću primene;
- utvrđuje jasne rokove za prikupljanje dokaza;
- osnovi za odbijanje su ograničeni;
- smanjuje administrativno opterećenje kroz uvođenje jedinstvenog standardnog obrasca;
- obezbeđuje zaštitu osnovnih prava odbrane.

Jasno je da se neke mere mogu proširiti samo ako su deo sveobuhvatnog skupa zajedničkih pravnih pravila. Međutim, države ugovornice bi možda želele da razmotre koji specifični aspekti EIO mogu da funkcionišu van okvira EU. Ovo bi moglo da obuhvati saradnju između država potpisnica Konvencije Saveta Evrope o borbi protiv trgovine ljudima i Evropske konvencije o ljudskim pravima. Mere koje se tiču određivanja rokova za prikupljanje dokaza i smanjenja administrativnog opterećenja kroz uvođenje standardizovanih procedura potencijalno bi se mogle sprovesti bez suštinskih promena u nacionalnim pravnim sistemima. Može se predvideti i neki poboljšani, zajednički skup pravila, pod uslovom da država poštuje odredbe Evropske konvencije o ljudskim pravima.

*Dodatna pitanja u vezi sa UPP.* Dokazi koje su dostavile države ugovornice takođe ukazuju na izazove u obradi zahteva za UPP koji su rezultat nedostatka osoblja koje je adekvatno obučeno za sastavljanje i obradu takvih zahteva – kao i korišćenja zastarele tehnologije. Na primer, neke države su navele da ne koriste uvek sigurnu e-poštu i druge oblike elektronske korespondencije prilikom razmene dokumenata sa stranim partnerima. Razvijanje upotrebe bezbednih oblika elektronskih komunikacija, uključujući pravila i mere zaštite, i promovisanje njihovog usvajanja među svim državama ugovornicama, moglo bi donekle da doprinese poboljšanju međunarodne saradnje među državama. Pored toga, širenje praktičnih informacija o kontaktnim tačkama/namenskim jedinicama unutar države koje mogu poslužiti kao „privilegovani kontakt" u slučajevima trgovine ljudima, uključujući trgovinu ljudima posredstvom IKT, takođe može da olakša procedure.

### 2.3.2. Elektronski dokazi

Iako su izazovi u vezi sa pribavljanjem elektronskih dokaza često povezani sa UPP, priroda i relevantnost takvih dokaza predstavlja niz dodatnih izazova koje treba razmatrati odvojeno.

Kako su istakli austrijski i britanski nadležni organi, elektronski dokazi mogu da otežaju identifikaciju tačne lokacije podataka. Utvrđivanje države u čijoj su nadležnosti podaci nije uvek jednostavno – što otežava izradu nacrta zahteva za uzajamnu pravnu pomoć. Portugalski nadležni organi smatraju da sistem za pribavljanje elektronskih dokaza iz drugih država nije „prikladan za svoju namenu", i navedeno je da Drugi dodatni protokol uz Budimpeštansku konvenciju (visokotehnološki kriminal)[15] može da donese unapređenja postojećeg sistema. Slično tome, grčki nadležni organi su pozvali na uspostavljanje zajedničkog pravnog okvira za brzu razmenu digitalnih dokaza (uz napomenu da postoji zajednički pravni okvir za očuvanje dokaza).

Otvoreno je pitanje o vremenu kada se zakonski može podneti zahtev za dostavljanje elektronskih dokaza. Prema britanskim nadležnim organima, „ponekad organi za sprovođenje zakona zahtevaju pristup sadržaju komunikacije pre nego što mogu da pokažu opravdani povod, ali preduslov za dobijanje takve pomoći mora da bude zadovoljen pre nego što se sadržaj podeli". Ovo naročito utiče na rane faze istrage. Slično tome, austrijski nadležni organi su naveli izazov koji podrazumeva „visoki prag potreban za dobijanje podataka o sadržaju od nekih država". Isti organi su pokrenuli pitanje koje vrste informacija je moguće tražiti tokom istrage i po kom pravnom osnovu (npr. sa ili bez sudskog naloga). Austrijski nadležni organi su pozvali na primenu „standardizovanog pristupa CID informacijama tokom istraga trgovine ljudima" (npr. traženje informacija o pretplatnicima od operatera mobilnih mreža). Oni su istakli da je „u nekim državama [ovo] moguće samo nakon što nadležni sud pošalje evropski nalog za istragu. U Austriji je to moguće bez sudskog naloga tokom istraga CID".

Kao što je već navedeno ranije u ovom izveštaju (odeljak 2.1.6), pravila o dužini čuvanja podataka su označena kao naročito problematična. Nekoliko država je izrazilo zabrinutost zbog nepostojanja homogene regulative o čuvanju podataka – čime se ometa razmena elektronskih dokaza. Neke države možda nemaju zakone o čuvanju podataka.

Konačno, nekoliko država je izrazilo zabrinutost zbog pristupa elektronskim dokazima koji se nalaze na računarskim serverima izvan njihove nadležnosti. Iskustva u ovom pogledu variraju u zavisnosti od države i kompanije koja poseduje podatke. Međutim, postoje brojni dokazi o poteškoćama u identifikaciji kompanije, njenom lociranju, uspostavljanju saradnje i organizovanju prenosa dokaza. Države ugovornice su izrazile potrebu za sveobuhvatnijim okvirom koji uređuje čuvanje i prenos elektronskih dokaza, kao i za zajedničkim pravnim okvirom koji zamenjuje postojeće ad hoc bilateralne radne sporazume između države i privatne kompanije koja drži podatke.

## 2.4. Izazovi tokom saradnje sa privatnim kompanijama

Studija je istraživala izazove sa kojima se države ugovornice suočavaju u borbi protiv trgovine ljudima kada rade sa IKT kompanijama i pružaocima internet usluga, uključujući pružaoce sadržaja i društvene medije. Iako se neki od ovih izazova preklapaju sa pitanjima o kojima

15 Drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu koji je usvojio Komitet ministara Saveta Evrope – Vesti (coe.int)

je već bilo reči, ipak je korisno ponuditi neka dalja razmatranja o problemima koja su istakle države ugovornice. U nastavku je dat pregled takvih izazova:

- Dobijanje blagovremenog odgovora od ISP i pružalaca sadržaja. Obraćanje pružaocima putem molbi poslatih preko relevantnih organa može dovesti do dugog čekanja sa rizikom da sadržaj bude izbrisan do trenutka kada se postupi po zahtevu. Francuski nadležni organi su istakli dugo vreme potrebno za odgovor na zahteve za dostavljanje metapodataka u vezi sa nalozima povezanim sa počiniocima; za podatke o sadržaju često treba da postoji zahtev za uzajamnu pravnu pomoć, za koji je potrebno po nekoliko meseci da se realizuje pošto se kompanije često nalaze izvan nadležnosti države koja upućuje zahtev (i Evropske unije).
- Pojašnjavanje pravnih zahteva u skladu sa kojima IKT kompanije i pružaoci internet usluga funkcionišu. Austrijski nadležni organi su izrazili zabrinutost da „međunarodni pružaoci usluga često nameću formalističke, pravno neopravdane zahteve agencijama za sprovođenje zakona kao preduslove za pružanje informacija i predaju korisničkih podataka i sadržaja. Izvršavanje naloga tužilaštva je ponekad veoma komplikovano". Prema tvrdnjama nadležnih organa iz Belgije, odbijanja često nisu adekvatno opravdana i objašnjena. Nadležni organi Bosne i Hercegovine su ukazali na poteškoće u dobijanju podataka koji nisu podaci o ličnosti tokom istraga (pre nego što se može izdati sudski nalog). Identifikacija ISP sama po sebi može da predstavlja izazov – kako su istakli nadležni organi Finske.
- Francuski nadležni organi su istakli probleme u vezi sa nepriznavanjem tužilaštva kao nezavisnog sudskog organa prilikom izdavanja zvaničnog zahteva za traženje podataka; dodatni problem su zahtevi kompanija da obelodane veliku količinu dokaza iz istrage koja je u toku pre nego što pravna služba kompanije može da donese odluku o predaji podataka.
- Belgijski nadležni organi su primetili nedostatak povratnih informacija o internim operacijama koje sprovode kompanije, npr. u vezi sa uklanjanjem sadržaja. Takođe su prijavili poteškoće u komunikaciji sa kompanijama – koje su često praćene čestim promenama osoblja za kontakt.
- Kao što je već navedeno, države su kao ključne izazove navele nedostatak usaglašenog zakonodavstva oko čuvanja podataka i neadekvatne zakonske odredbe. U Norveškoj, na primer, ISP-ovima nije dozvoljeno da čuvaju podatke o IP adresama duže od 21 dan i od njih se ne traži da čuvaju podatke o vezi između pretplatnika i IP adrese. Prema norveškim nadležnim organima, to „otežava policiji da identifikuje osumnjičene za trgovinu ljudima posredstvom IKT". Ovaj problem se pogoršava kada se radi o kompanijama koje su osnovane da pružaju anonimne i šifrovane usluge.
- Moldavski nadležni organi su prijavili nedostatak određene kontakt tačke u privatnim kompanijama koje upravljaju društvenim medijima i drugim aplikacijama za umrežavanje. Predloženo je da se uspostavi kontaktna tačka za svaku državu/područje (u zavisnosti od broja korisnika). (Može se misliti i na kontaktne tačke određene na osnovu jezika koji se govori). Moldavski nadležni organi su predložili da uspostavljanje kontaktnih tačaka bude obavezno za ISP, pružaoce sadržaja i društvene medije. Slovački nadležni organi su istakli problem jezičkih veština u kompanijama, jer su primetili da velikim kompanijama koje posluju u više država često nedostaje osoblje koje poseduje jezičke i pravne veštine relevantne za svaku državu u kojoj posluju.
- ISP-ovima nije uvek jasno koje su nacionalne agencije odgovorne za određene odluke, npr. uklanjanje nezakonitog sadržaja. Slovački nadležni organi su predložili da se uvede uloga „pouzdanog čuvara sadržaja", odnosno da se identifikuju određene agencije koje imaju zadatak da se povezuju sa međunarodnim pružaocima usluga kako bi uklonili sadržaje i postupali po drugim zakonskim odredbama. Pouzdani čuvar sadržaja bi imao otvoren kanal komunikacije sa kompanijama i izgradio bi uzajamno poverenje.

Nekoliko država, uključujući Kipar, Irsku, Letoniju, Luksemburg, Maltu, Holandiju i Ujedinjeno Kraljevstvo, navelo je da su ISP-ovi, pružaoci sadržaja i kompanije društvenih medija generalno sarađivali kada se radi o pitanjima koja su vezana za trgovinu ljudima i seksualnu eksploataciju dece. Međutim, britanski nadležni organi su istakli potrebu da se napravi korak dalje i sarađuje sa onlajn kompanijama „na **osmišljavanju mogućnosti** za trgovinu ljudima na njihovim veb lokacijama i radu u saradnji sa organima za sprovođenje zakona kako bi se sprečila pojava trgovine ljudima".

Kiparski nadležni organi su naveli korišćenje platforme Sirius za olakšavanje prekograničnog pristupa elektronskim dokazima koji vodi Evropol kao primer dobre prakse. Takva platforma daje agencijama za sprovođenje zakona mogućnost da direktno komuniciraju sa privatnim kompanijama radi čuvanja i obelodanjivanja podataka. Ovo su istakli i francuski nadležni organi (Projekat E-Evidence).

## 2.5. Dokazi prikupljeni od NVO

Pored dokaza prikupljenih od država ugovornica, u okviru studije se od NVO koje pružaju pomoć žrtvama tražilo da ukažu na izazove koje primećuju u kontekstu trgovine ljudima posredstvom tehnologije.

### 2.5.1. Izazovi tokom identifikacije i istrage

Sve u svemu, dokazi prikupljeni od NVO su u skladu sa izazovima koje su navele države ugovornice i o kojima je bilo reči ranije u ovom poglavlju. Konkretnije, NVO su istakle sledeći skup faktora koji ometaju otkrivanje trgovine ljudima posredstvom tehnologije i naknadne istrage:

- Nedostatak kapaciteta među organima za sprovođenje zakona, uključujući nedostatak obuke, hardvera i softvera, kao i ograničenu upotrebu specijalnih istražnih tehnika. Neke NVO su primetile nedostatak specijalizacije policije i pravosuđa u pogledu trgovine ljudima u vezi sa tehnologijom, kao i nedostatak kapaciteta u oblasti velikih količina podataka. Međutim, alati za „struganje" interneta koje je isprobala organizacija Hope Now (Danska) u periodu 2016–2018 postigli su skromne rezultate.
- Tehnološko okruženje koje se brzo menja, kao i modus operandi počinilaca. Profesionalcima je teško da prate korak sa trgovinom ljudima posredstvom tehnologije, što ometa njihovu sposobnost da brzo identifikuju slučajeve i pokreću istrage. Znanje o tehničkom okruženju i praksama često se ne razmenjuje (npr. među organima za sprovođenje zakona, privatnim kompanijama, NVO, akademskom zajednicom).
- Korišćenje privatnih foruma, soba za ćaskanje ili šifrovanih aplikacija za kontakte između počinilaca i žrtava. Ovo otežava (a) otkrivanje takvih kontakata i (b) njihovo pribavljanje kao dokaza koji će se koristiti na sudu. NVO su predložile navođenje informacija/upozorenja o bezbednom korišćenju privatnih kanala komunikacije.
- Poteškoće u razotkrivanju anonimnih počinilaca tokom emitovanja eksploatacije uživo putem interneta, kao i poteškoće u prikupljanju dokaza o takvim zlostavljanjima, osim ako se ne naprave snimci ekrana predmetnih video snimaka.
- Profesionalci smatraju da je teško utvrditi da li osoba koja stoji iza onlajn profila/oglasa dobrovoljno pruža navedene usluge na osnovu javno dostupnih informacija (npr. u slučaju onlajn oglasa za seksualne usluge). To je zato što počinioci mogu da kreiraju i upravljaju onlajn profilima u ime svojih žrtava. Štaviše, počiniocima je lako da ponovo kreiraju profile kada im se zabrani pristup.

- Pravila o zaštiti podataka i privatnosti mogu da ometaju identifikaciju žrtava, kao i trgovaca ljudima. Pravila GDPR ograničavaju upotrebu tehnologije za otkrivanje digitalnih tragova koje ostavljaju i žrtve i počinioci (na društvenim medijima, na internetu, ali i u vezi sa finansijskim računima). Nedostaje sveobuhvatna analiza digitalnih tragova usredsređena na žrtve, uključujući, na primer, nekretnine, bankovne račune, transakcije na bankomatima, transakcije kreditnim karticama i medicinske kartone, kako bi se olakšala istraga.
- Nedostatak interdisciplinarne tehnološke saradnje između privatnih kompanija, javnih agencija i NVO kako bi se u potpunosti iskoristila sve veća količina podataka o trgovini ljudima. Fondacija Sustainable Rescue Foundation je navela sledeće faktore koji ometaju međusektorsku saradnju u pogledu razmene podataka:
    - nezavisni centri ne uspevaju da privuku agencije za sprovođenje zakona ili vladu;
    - nedostatak tehnološke strategije u nacionalnim akcionim planovima za borbu protiv trgovine ljudima;
    - IT grupe pri organima za sprovođenje zakona koje nemaju kapacitet ili budžet za blagovremeni razvoj, testiranje, implementaciju, obuku, ažuriranje i održavanje aplikacija za otkrivanje trgovine ljudima;
    - poteškoće oko deljenja podataka o žrtvama;
    - komercijalni interesi.
- Ograničene istrage finansijskih institucija o trgovini ljudima. Mogućnosti identifikacije na osnovu podataka iz sistema Upoznaj svog klijenta(KYC) se ne koriste zbog nedostatka obuke i svesti o trgovini ljudima, kao i zbog složenosti sistema prijavljivanja (kvalitet upozorenja, veoma veliki broj lažno pozitivnih prijava, dugo vreme potrebno za odgovor itd.)
- Nedostatak ulaganja u sposobnosti veštačke inteligencije (AI) i korišćenje mašinskog učenja za operacije, predviđanje i prevenciju. Fondacija Sustainable Rescue Foundation je ukazala na upotrebu mašinskog učenja u medicinskom sektoru kao na primer gde se „informacije dele između klinika, bolnica, lekara i akademske zajednice bez kršenja zakona o privatnosti. Ovo se postiže korišćenjem načela FAIR pri pregledu podataka (engleski akronim dobijen od termina: vidljivi, pristupačni, interoperabilni, ponovo upotrebljivi) za podudaranje metapodataka i spoljašnjeg učenja za dubinsku analizu iz različitih izvora". Takođe su istakli da „trenutno nije u toku takvo ulaganje ili takva strategija u organizacijama za trgovinu ljudima".
- Nedostatak razmene podataka između različitih subjekata na lokalnom, regionalnom, nacionalnom ili međunarodnom nivou zbog nedostatka operativnih sposobnosti u okviru organa za sprovođenje zakona i ograničenja utvrđenih nacionalnim zakonodavstvom. Pored toga, podaci se često prikupljaju u nestrukturisanom obliku, što otežava razmenu i dalju analizu dokaza.
- NVO koje pružaju direktnu podršku žrtvama trgovine ljudima, putem onlajn platformi, konsultacija putem ćaskanja i telefonskih linija za pomoć, nemaju kapacitete, resurse i tehničke alate da redovno otkrivaju onlajn eksploataciju koja se vrši posredstvom tehnologije.
- Nedostatak svesti o rizicima i potencijalnim posledicama u vezi sa upotrebom tehnologije među ljudima koji su u opasnosti od trgovine ljudima. Ovo je naročito akutno kod dece i mladih. Uopšteno govoreći, postoji nedostatak svesti u široj javnosti o trgovini ljudima posredstvom tehnologije, što dovodi do nedovoljnog prijavljivanja.

### 2.5.2. Izazovi saradnje sa organima za sprovođenje zakona

Sve NVO prijavljuju neki oblik saradnje sa agencijama za sprovođenje zakona, uključujući signaliziranje slučajeva trgovine ljudima ili pružanje pomoći žrtvama na zahtev nadležnih organa. Kada je reč o njihovoj saradnji sa organima za sprovođenje zakona, NVO su istakle sledeće izazove:

- Suprotstavljeni ciljevi ili različiti pristupi između NVO i organa za sprovođenje zakona, uključujući odluke o tome da li slučaj treba dalje istraživati.
- Pitanja koja se tiču zaštite i privatnosti podataka.
- Nedostatak povratnih informacija o slučajevima koje su NVO prijavile nadležnim organima.
- Nedostatak resursa za podršku saradnji između organa za sprovođenje zakona i NVO (ovo je istaknuto i u vezi sa inovativnim „terenskim laboratorijama" uspostavljenim u Holandiji, u čijim odborima je fondacija Sustainable Rescue Foundation).
- Kada je reč o deci, postoji nedostatak obuke među organima za sprovođenje zakona o tome kako da pristupe maloletnim žrtvama i da ih ubede da sarađuju tokom istrage. La Strada Moldova je istakla da istrage koje uključuju decu imaju dodatnu složenost kada je reč o upravljanju dokazima, jer „deca obično osećaju krivicu, prekor ili stid zbog onoga što im se desilo, ne sarađuju, ne žele da roditelji saznaju šta im se desilo ili da druge osobe vide njihove seksualno eksplicitne video materijale. U strahu, mnoga od njih odbijaju da podnesu pritužbu", čime onemogućavaju dalju istragu agencija za sprovođenje zakona.

## 2.6. Tehnološke kompanije

Kompanija Facebook je navela da korisnici „retko prijavljuju" sadržaje koji se odnose na trgovinu ljudima. Kompanija je dalje primetila da nedovoljno prijavljivanje može biti posledica brojnih faktora, uključujući: (a) žrtve trgovine ljudima možda nemaju slobodu da prijave ili možda nisu svesne svojih uslova eksploatacije; (b) kupci usluga koje pruža žrtva trgovine ljudima možda nisu svesni da kupuju uslugu od žrtve trgovine ljudima ili su odvraćeni od prijavljivanja „jer žele da iskoriste nedozvoljene ili znatno jeftinije usluge koje se pružaju eksploatacijom". U drugim slučajevima, primećuje se da „za određene oblike trgovine ljudima, kao što je kućno ropstvo, pošto to može biti opšteprihvaćena pojava u nekim regionima, posmatrači ne shvataju da mogu ili da treba da prijave ovakve sadržaje".

Što se tiče izazova za saradnju sa organima za sprovođenje zakona, IBM je primetio da postoji „određeni broj prepreka"; pre svega, istakao je „zabrinutost u pogledu zakonitosti takve saradnje, naročito u vezi sa pitanjima privatnosti podataka i pravnom složenošću situacije u kojoj nadležnost ima više država". IBM je pozvao na „pojašnjenja o međunarodnim pravnim dozvolama za prikupljanje i deljenje podataka (sa ovlašćenim organima za sprovođenje zakona)". Facebook je naveo da prekogranična priroda eksploatacije ljudi „predstavlja izazov". Na primer, napomenuo je da počinioci mogu da se nalaze u drugoj državi od one u kojoj se nalaze žrtve trgovine ljudima i zlostavljana lica: shodno tome, „više država može da bude nadležno za vođenje istrage protiv kriminalne mreže. Koordinacija između organa za sprovođenje zakona u EU i šire dodaje dodatnu složenost naporima u borbi protiv trgovine ljudima".

## 2.7. Dodatni dokazi prikupljeni na osnovu analize okruženja

Pored dokaza koje su pružile države ugovornice, NVO i tehnološke kompanije, u okviru studije je takođe sprovedeno kancelarijsko istraživanje dostupne baze dokaza o izazovima u vezi sa otkrivanjem, istragom i krivičnim gonjenjem slučajeva trgovine ljudima posredstvom interneta i tehnologije.

Od posebnog interesa su dokazi koji se odnose na izazove pri **identifikaciji oglasa za posao povezanih sa trgovinom ljudima**. Predloženo je da bi identifikacija oglasa, a ne žrtava, mogla da predstavlja dobar način da se iskoristi tehnologija: ovo seže do podsticajnih radova SE (2007) i projekta Fine Tune (2011). Projekat Fine Tune (2011) ponudio je preliminarnu listu **znakova upozorenja u kontekstu radne eksploatacije**. To uključuje: (a) nerealno visoke plate za nekvalifikovane poslove; (b) opise poslova bez detalja, uključujući opis uloge, lokacije, mesta rada i dnevnog radnog vremena; (c) odsustvo adrese kompanije ili agencije koja zapošljava; i (d) odsustvo kontakt podataka osim broja telefona ili generičke adrese e-pošte. Međutim, dokazi ukazuju da je identifikacija pravih pozitivnih slučajeva (tj. oglasa u vezi sa trgovinom ljudima) i dalje veoma izazovna. Nekoliko autora je ukazalo na **poteškoće u sortiranju** pravih oglasa od onih koji se odnose na trgovinu ljudima, uprkos naporima uloženim u razvoj **indikatora potencijalnog rizika** (kao i ponovnom tumačenju opštih indikatora UNODC-a i MOR-a kako bi se prilagodili onlajn kontekstu: Di Nicola i drugi 2017; Raets i Janssens 2018; Volodko i drugi 2019):

a. U skupu od 430 litvanskih onlajn oglasa za posao koje su analizirali Volodko i drugi (2019), 98,4% sadržalo je najmanje jedan indikator trgovine ljudima, što ukazuje na to da su takvi indikatori često uobičajena karakteristika tržišta rada sa niskim kvalifikacijama. Određeni nivo nade, međutim, potiče iz nalaza da je samo 15% oglasa sadržalo više od pet indikatora, što ukazuje na to da bi se uz dalje usavršavanje i odgovarajuće analitičke tehnike neke strategije za smanjenje štete mogle efikasno primeniti.
b. Pored usavršavanja dostupnog skupa znakova upozorenja (i njihovog stalnog ažuriranja, što predstavlja dodatni izazov), kao potencijalni put napred predloženi su računarski pristupi zasnovani na „struganju" interneta, obrada prirodnog jezika, prepoznavanje subjekata i „oznaka" i uopšteno tehnike mašinskog učenja (Volodko i drugi 2019, između ostalih; takođe videti UN Delta 8.7). Iako potencijalno obećava, ovaj put otvara nove izazove, uključujući: (1) potrebu da se utvrdi „osnovna istina" za modele, što se može postići samo kroz blisku saradnju između agencija za sprovođenje zakona i privatnog sektora; (2) potrebu da se iskoristi znanje iz privatnog sektora, pošto agencije za sprovođenje zakona interno jedva da imaju potrebne veštine; (3) potrebu da se pažljivo procene etička pitanja u vezi sa tehnikama mašinskog učenja velikih razmera; i (4) potencijal za diskriminatorne prakse, kao i pitanja zaštite podataka i razmene informacija između različitih subjekata.

U nekim slučajevima, oglasi za posao u modelingu, zabavi i – u nekim državama – seksualnim uslugama u inostranstvu mogu se koristiti za regrutovanje pojedinaca koji potom bivaju primorani na seksualnu eksploataciju. Predloženo je nekoliko znakova upozorenja kako bi se oglasi u vezi sa trgovinom ljudima odvojili od legitimnih oglasa, uključujući oglase koji: (a) su loše napisani i nejasni; (b) previše obećavaju; (c) su preširoki; (d) ne navode državu odredišta (upućuju na „egzotične destinacije"); i (e) ne sadrže puno ime kontakt osobe, agencije za zapošljavanje i/ili kompanije koja bi zaposlila uspešnog kandidata (Di Nicola i drugi 2017). Međutim, preliminarni pokušaji da se pregledaju javno dostupni dokazi korišćenjem ovih kriterijuma još jednom su ukazali na poteškoće u odvajanju oglasa povezanih sa trgovinom ljudima od lažno pozitivnih oglasa.

Otkrivanje slučajeva seksualne eksploatacije na osnovu **onlajn oglasa za seksualne usluge** je podjednako izazovno, tj. razvrstavanje seksualnih usluga koje pružaju žrtve trgovine ljudima od onih koje pojedinci dobrovoljno pružaju na osnovu jedinstvenog teksta i vizuelnih prikaza uključenih u oglas. Predloženi su neki indikatori eksploatacije, uključujući neslaganja između opisa profila, slika i lokacija; takva neslaganja se takođe mogu unakrsno proveriti na više veb lokacija (Di Nicola i drugi 2017). Pokazalo se da brojevi telefona igraju ključnu ulogu, na primer, u otkrivanju prisustva istog broja telefona u oglasima, na veb lokacijama i objavama koje se pripisuju različitim osobama (potencijalan znak upozorenja). Predloženo je da se prepoznavanje lica može koristiti kao tehnika za uočavanje nedoslednosti i znakova upozorenja, slično pristupu usvojenom u otkrivenim seksualnim materijalima koji prikazuju maloletnike (Raets i Janssens 2018).

Međutim, preliminarni pokušaji da se proširi gore navedena strategija otkrivanja ukazali su na jasne izazove. U svojim pokušajima da identifikuju žrtve seksualne trgovine u SAD putem onlajn oglasa za poslovnu pratnju, Ibanez i Ganzan (2014, 2016a i 2016b) koristili su brojeve telefona i indikatore kretanja, ali nisu dali jake rezultate. Pored toga, neki od indikatora koje su naveli Ibanez i Gazan 2014. su prilično zbunjujući i možda uopšte ne ukazuju na trgovinu ljudima; u nekim slučajevima, oni mogu čak da ukazuju na suprotnu situaciju.

# 3. Strategije i dobre prakse

Nakon razmatranja izazova, studija se sada okreće istraživanju strategija koje su države ugovornice razvile za otkrivanje i istragu trgovine ljudima posredstvom interneta i tehnologije, za negovanje međunarodne saradnje, i za identifikaciju i pomoć žrtvama. Zatim sledi diskusija o dokazima koje su pružile NVO i tehnološke kompanije o istim problemima.

## 3.1. Otkrivanje slučajeva trgovine ljudima posredstvom IKT

### 3.1.1. Opšte strategije

Države su navele da primenjuju različite strategije za otkrivanje slučajeva trgovine ljudima posredstvom interneta i IKT. Često se navodi strategija **nadgledanja interneta**, uključujući foruma i, u nekim slučajevima, TOR mreže (mračne mreže). Ovo se često kombinuje sa upotrebom **obaveštajnih podataka iz otvorenih izvora (OSINT)**, veoma čestom istražnom strategijom koja podrazumeva prikupljanje podataka sa društvenih medija i iz drugih javno dostupnih onlajn izvora o mreži kontakata određenog pojedinca, njegovim životnim uslovima i finansijskoj situaciji. OSINT se može koristiti „proaktivno", npr. za otkrivanje potencijalnih slučajeva trgovine ljudima, za identifikaciju potencijalnih počinilaca i žrtava ili za pribavljanje svežih informacija. Neke države su formirale **„sajber patrole" sa specijalizovanim službenicima** zaduženim za sprovođenje OSINT istraga na internetu. Neke države dozvoljavaju tajne istrage na internetu (sajber infiltracija). U Holandiji, specijalizovani istražitelji sa „**digitalnim znanjem**" mogu da budu angažovani u istragama trgovine ljudima kako bi prikupili onlajn dokaze o trgovini ljudima. Finski nadležni organi su ukazali na nedavno uspostavljanje podjedinice za borbu protiv trgovine ljudima na internetu u okviru Nacionalnog istražnog tima (takođe su prijavili prisustvo ogranka za onlajn obaveštajnu delatnost koji radi na internetu, uključujući mračnu mrežu).

Vezano za OSINT istrage, države navode da koriste **tehnike analize društvenih mreža** kako bi se razumele i rekonstruisale mreže kontakata počinioca i/ili žrtve. Primera radi, ako je žrtva A povezana sa osobom koja vrši regrutovanje B, onda se mogu proceniti svi kontakti osobe koja vrši regrutovanje B kako bi se identifikovale potencijalne žrtve. **Informacije o povezanostima** su ključne i sve više ih koriste policijski organi kroz takozvanu „analizu veza" ili sofisticiranije tehnike „analize društvenih mreža".

Dodatne **proaktivne strategije** uključuju upotrebu tehnoloških alata za traženje dokaza na mreži (npr. sistemi za skeniranje mreže, videti takođe u nastavku) i strateške istrage o *modus operandiju* počinilaca u oblasti trgovine ljudima u pogledu IKT. Generisanje – i ažuriranje – ovakvog strateškog (šireg) znanja o toj pojavi može da pruži informacije za holistički pristup, kao i za specifične, usmerenije istrage. Međutim, nisu sve države ugovornice navele da koriste „strategije". Nekoliko država ugovornica je izričito navelo da njihove istrage o trgovini ljudima posredstvom IKT ostaju „reaktivne".

Nadležni organi su prijavili uspostavljanje direktnog kontakta sa pružaocima onlajn usluga kako bi se identifikovali slučajevi trgovine ljudima posredstvom IKT. U državama u kojima je oglašavanje seksualnih usluga na mreži zakonito, nadležni organi mogu da „izvrše ciljano filtriranje telefonskih brojeva i [analizu] korisničkih podataka povezanih sa [pretpostavljenim] počiniocima" (prijava iz Mađarske). Kantonalne policijske snage u Švajcarskoj vrše „ciljane provere" onlajn oglasa za seksualne usluge kako bi otkrile potencijalne žrtve trgovine ljudima.

Neki agencije za sprovođenje zakona u Ujedinjenom Kraljevstvu koriste **alate za „struganje" interneta** posebno razvijene za izdvajanje informacija sa veb lokacija kako bi identifikovale rizike i ranjivosti na veb lokacijama za usluge za odrasle (ASW). Britanske policijske snage vrše pregledanje veb lokacija za ASW kako bi prikupile podatke koji se potom koriste za analizu aktivnosti na ASW i potencijalno pretvaranje ovih podataka u obaveštajne podatke po kojima se može delovati.

Nekoliko država je navelo dostupnost **mehanizma za korisnike interneta da prijave sadržaje i veb lokacije** za koje sumnjaju da su povezani sa nezakonitim aktivnostima, uključujući seksualnu i radnu eksploataciju (videti u nastavku za više primera).

### 3.1.2. Strategije specifične za određenu državu

Kako bismo dalje istražili različite strategije koje su države razvile za borbu protiv zloupotrebe interneta, uključujući onlajn oglase za posao, u kontekstu trgovine ljudima posredstvom tehnologije, sada donosimo kratak pregled mehanizama i inicijativa specifičnih za određenu zemlju. Takve strategije treba čitati zajedno sa dobrim praksama o kojima se govori u sledećem odeljku, kao i sa raspravom o nacionalnim pravnim okvirima koji se odnose na identifikaciju i uklanjanje internet sadržaja u vezi sa trgovinom ljudima koji su uključeni u Veb prilog. U Albaniji postoji **mehanizam dozvola** u vezi sa onlajn oglasima za posao, a njih izdaju/kontrolišu institucije (koje nisu navedene u prijavi).

Austrijski nadležni organi su intenzivirali proaktivne pretrage na različitim onlajn platformama od izbijanja kovida-19 kako bi identifikovali žrtve i počinioce trgovine ljudima koristeći **posebne softverske tehnologije** (npr. sisteme za skeniranje mreže radi prikupljanja podataka), **službenike specijalizovane za obaveštajne podatke iz otvorenih izvora** (OSINT), kao i **tajne agente** (tajne istrage na internetu). Aktivnosti zajednički sprovode istražitelji za trgovinu ljudima i službenici specijalizovani za IT. Veruje se da bi ovaj model mogao da ponudi šablon za buduće istrage.

Belgijski nadležni organi su naveli da trenutni „abolicionistički model" usvojen u vezi sa prostitucijom onemogućava zaključivanje ugovora sa veb lokacijama koje objavljuju oglase za seksualne usluge. Ovo se smatra „ograničenjem" postojećeg zakonodavstva. NVO „Child focus" trenutno razvija kampanju za podizanje svesti za klijente koji koriste veb lokacije na kojima se objavljuju oglasi za seksualne usluge, kako bi bili obavešteni o riziku da naiđu na maloletnu osobu. Ova kampanja se sprovodi u saradnji sa predmetnim veb lokacijama.

Hrvatski nadležni organi su prijavili da vrše **provere profila na društvenim mrežama** pojedinaca koji su povezani sa konkretnim krivičnim istragama, npr. istragama seksualnog zlostavljanja i seksualne eksploatacije dece, kako bi se identifikovale potencijalne žrtve i osobe koje vrše regrutovanje. Takve provere vrše specijalizovani službenici za visokotehnološki kriminal.

Na Kipru postoje kampanje za podizanje svesti koje organizuje Odeljenje za visokotehnološki kriminal (CCD), a koje su namenjene školskoj deci i njihovim roditeljima kao deo Nacionalne strategije za bolji internet za decu. Od 2014. godine, CCD takođe vodi platformu za prijavljivanje visokotehnološkog kriminala (www.cyberalert.cy).

U Estoniji, građani mogu da kontaktiraju „**veb službenike**" kako bi prijavili sadržaj društvenih medija koji je potencijalno povezan sa nezakonitim aktivnostima, uključujući trgovinu ljudima.

Francuski zakon dozvoljava istražiteljima da se **sajber infiltriraju u kriminalne mreže.** Agencije za sprovođenje zakona zapošljavaju istražitelje za sajber patroliranje internetom kako bi **otkrili oglase i identifikovali kriminalne mreže.** Operacije ciljanog nadzora na određenim internet forumima se takođe sprovode, uz korišćenje tehnika tajne istrage gde je to potrebno. Istražitelji takođe koriste internet oglase za unakrsnu proveru geografskih podataka prikupljenih preko drugih izvora kako bi identifikovali mesta koja se koriste za trgovinu ljudima. Informacije prikupljene iz različitih izvora se sistematizuju i koriste za **rekonstrukciju kriminalnih mreža, odnosno odnosa između određenih mesta, počinilaca i žrtava**. Pored toga, francuske agencije za sprovođenje zakona rade na uspostavljanju **protokola saradnje** sa kompanijama koje upravljaju društvenim mrežama i onlajn privatnim platformama za iznajmljivanje kako bi podstakle pružanje informacija. Pošto pružaoci internet sadržaja mogu u nekim slučajevima da budu preopterećeni obimom zahteva za prenos informacija i dostavljanje dokaza, nadležni organi su predložili da se **osmisle direktnije – i pojednostavljene – procedure koje podržavaju saradnju** između pružalaca sadržaja i organa za sprovođenje zakona. Na primer, „Wannonce", francuska stranica koja se koristi za oglase povezane sa maloletnom prostitucijom, šalje organima za sprovođenje zakona vezu koja omogućava direktnu pretragu u njihovoj bazi podataka nakon dostavljanja adrese e-pošte. Konačno, član 6(I)(7) Zakona br. 2004–575 od 21. juna 2004. godine o „Poverenju u digitalnu ekonomiju" (LCEN) zahteva od pružalaca pristupa internetu i hostova veb lokacija da pomognu u borbi protiv širenja materijala koji se odnose na određena krivična dela, uključujući trgovinu ljudima. Od njih se zahteva da postave lako dostupan i vidljiv mehanizam koji omogućava svakoj osobi da označi sumnjivi materijal. Kompanije su takođe dužne da blagovremeno obaveste javne organe o svim nedozvoljenim radnjama koje su im prijavljene i koje sprovode korisnici njihovih usluga. Građani mogu da prijave nezakonite sadržaje na internetu policiji i žandarmeriji putem veb lokacije (www.internet-signalement.gouv.fr). Prijavljeni sadržaj ispituje PHAROS (*Plateforme d'Harmonisation*, *d'Analyse*, *de Recoupement et d'Orientation des Signalements*), specijalizovana policijska jedinica.

U Finskoj, služba za zaštitu dece i telefonska linija za prijavu (*Nettivihje*) nude način za prijavu onlajn materijala za seksualno zlostavljanje dece i trgovinu decom. *Nettivihje* blisko sarađuje sa Nacionalnim istražnim biroom i njegovim timom specijalizovanim za seksualne zločine. Finska policija takođe ima onlajn mehanizam za prijavu sumnjivih aktivnosti na internetu, uključujući materijale potencijalno povezane sa seksualnim prestupima nad decom. Ovaj obrazac se potencijalno može proširiti izvan domena seksualne eksploatacije dece.

U Nemačkoj, policija je (u maju 2020.) počela da koristi **alat za automatsko pretraživanje** za analizu velike količine podataka koji su objavljeni na veb lokacijama za oglase za odrasle. Alat za pretraživanje strukturiše podatke kako bi pomogao u izdvajanju relevantnih informacija. Ovo se postiže u kombinaciji sa upotrebom specifičnih indikatora. Nadležni organi smatraju da je upotreba ovog automatizovanog alata „veoma korisna".

Grčki nadležni organi pominju **praćenje veb lokacija i foruma koji objavljuju oglase za posao** ili usluge kako bi otkrili slučajeve trgovine ljudima na internetu. Ovo se postiže kroz blisku saradnju između Jedinica za borbu protiv trgovine ljudima Policije Grčke i Odeljenja za visokotehnološki kriminal. Pored toga, Odeljenje za visokotehnološki kriminal Policije Grčke razvilo je aktivnosti za podizanje svesti i edukaciju koje se fokusiraju na odgovornu upotrebu novih tehnologija i rizike na internetu, na primer, „Seminari za dan bezbednog surfovanja" i veb lokacija i aplikacija „Cyberkid", koja služi za informisanje učenika, roditelja i nastavnika o nasilju na internetu i rizicima sa kojima se oni mogu suočiti na veb lokacijama društvenih mreža. NVO „Smile of the Child" redovno organizuje događaje na Dan bezbednog interneta (9. februar).

Na Islandu, policija Rejkjavika održava takozvane „**nedelje interneta**", tokom kojih pregleda popularne veb lokacije koje reklamiraju seksualne usluge u potrazi za slučajevima trgovine ljudima. U slučaju sumnjivih aktivnosti, policija traži sudski nalog za prisluškivanje telefonskih brojeva navedenih u oglasima i pokretanje istrage.

U Irskoj, Jedinica za koordinaciju i istragu trgovine ljudima An Garda Síochána (Irske policije) udružuje snage sa različitim društvenim medijima i kompanijama za zapošljavanje kako bi podigla svest o potencijalnim oglasima za posao koji su povezani sa trgovinom ljudima. Irske i neke međunarodne IKT kompanije obično sarađuju kada An Garda Síochána zatraži uklanjanje sadržaja sa interneta za koji se smatra da je nezakonit.

U Letoniji postoji zvanična veb lokacija za oglase za posao koju vodi Državna agencija za zapošljavanje. Veb lokacija nastoji da spreči slučajeve radne eksploatacije **nudeći bezbedan prostor za oglašavanje.**

U Republici Moldaviji trenutno ne postoje posebni automatizovani mehanizmi za identifikaciju oglasa i sadržaja na internetu koji su potencijalno povezani sa trgovinom ljudima, a nadležni organi trenutno sarađuju sa Holandijom na nabavci sistema za skeniranje mreže koji su razvili holandski organi za sprovođenje zakona.

U Holandiji, **policija može da postavi lažne profile na internetu** (lokprofiel) kako bi identifikovala – a zatim istražila – slučajeve trgovine ljudima i počinioce. Pored toga, Ministarstvo pravde i bezbednosti trenutno istražuje ulogu tehnologije u svim fazama trgovine ljudima kroz stručne sastanke i istraživanja koja se sprovode u saradnji sa Centrom za borbu protiv eksploatacije dece i trgovine ljudima (CKM).

U Norveškoj, Centar za visokotehnološki kriminal trenutno razvija **bazu podataka o seksualnim oglasima na internetu** koji su objavljeni na lokalnoj veb lokaciji. Takve informacije će pružiti osnovu za dalju analizu.

U Sloveniji je 2005. godine osnovan Centar za bezbedniji internet kako bi se podigla svest i pomoglo u otkrivanju nezakonitih sadržaja na internetu. Centar nudi tri glavne usluge: (a) **centar za podizanje svesti** o odgovornom korišćenju interneta i novih tehnologija (Safe.si) koji ima za cilj da deci, tinejdžerima, roditeljima, nastavnicima i socijalnim radnicima pruži onlajn/oflajn aktivnosti, obrazovanje, radionice, sadržaje, kampanje za podizanje svesti; (b) telefonsku liniju za pomoć deci, mladima i roditeljima (takođe poznat kao „Tom telefon") sa profesionalnim savetnicima koji nude savete o bezbednosti na internetu, takođe i putem **sobe za ćaskanje na internetu**; (c) anonimno onlajn prijavljivanje nezakonitog sadržaja na internetu.

U Španiji, nadležni organi koriste **praćenje društvenih medija** posredstvom sajber patrola koje su fokusirane na otkrivanje žrtava trgovine ljudima. Ove aktivnosti sprovodi Centralna istražna jedinica Guardia Civil specijalizovana za trgovinu ljudima, a same aktivnosti su intenzivirane tokom pandemije kovida. Policía National je takođe nedavno osnovala istražnu grupu specijalizovanu za slučajeve trgovine ljudima na internetu (Operativna grupa VI za borbu protiv sajber trgovinu ljudima sa Centralnom brigadom Policía Nacional za borbu protiv trgovine ljudima).

U Švedskoj, policija vrši **redovan nadzor veb lokacija** koje oglašavaju aktivnosti prostitucije kako bi se identifikovalo mesto i vreme takvih aktivnosti (prema švedskom zakonu, sve kupovine seksualnih usluga su nezakonite).

U Švajcarskoj, neke kantonalne policijske snage koriste **tajne istrage za proveru oglasa** na veb lokacijama za odrasle, kao i pojedince koji su uključeni u otkrivanje slučajeva trgovine ljudima.

U Ujedinjenom Kraljevstvu, Agencija za borbu protiv zlostavljanja na radu i organizovanog kriminala, zajedno sa organizacijom Crimestoppers, koristila je Facebook da informiše tražioce posla o lažnom oglašavanju poslova na društvenim medijima. Tim je **kreirao oglase za posao na mreži Facebook** koji su pružali hipervezu ka veb lokaciji organizacije Crimestoppers, koja je zauzvrat pružala informacije o indikatorima rizika pri traženju posla u građevinskoj industriji. Kampanja je bila usmerena na Rumune starosti od 18 do 34 godine i dosegla je preko 900.000 ljudi. Došlo je do povećanja od 13% u prijavama koje se odnose na trgovinu ljudima i od 400% u prijavama o trgovini ljudima koje se odnose na žrtve iz Rumunije. U okviru višeagencijskog pristupa (projekat AIDANT) koji okuplja Nacionalnu agenciju za borbu protiv kriminala, Granične snage, Imigracione službe, Poresku službu i carinu Njenog Veličanstva, Agenciju za borbu protiv zlostavljanja na radu i organizovanog kriminala i policijske snage, nadležni organi **smišljaju i testiraju nove metodologije za prijavljivanje u industriji**. Jedinica NCA za borbu protiv trgovine ljudima u svrhu modernog ropstva (MSHTU) radi na podizanju standarda na veb lokacijama za usluge za odrasle (ASW) tako što poboljšava način na koji kompanije identifikuju trgovinu ljudima i eksploataciju na svojim platformama i prijavljuju to organima za sprovođenje zakona. Policijske snage takođe koriste automatizovane istraživačke procedure iz otvorenih izvora za prikupljanje informacija iz oglasa na veb lokacijama za usluge za odrasle (ASW). Britanski nadležni organi smatraju da je gašenje ASW rizično, jer verovatno neće dovesti do eliminacije potražnje, ali bi umesto toga dovelo do izmeštanja oglašavanja na druge platforme na štetu žrtava trgovine ljudima i dobrobiti seksualnih radnika. Pored toga, razvijena je aplikacija Farm Work Welfare sa ciljem da se dopre do sezonskih radnika i poslodavaca u sektoru poljoprivrede i proizvodnje hrane, a postavljena je i glasovna šema za radnike (SAFERjobs, www.safer-jobs.com) koja omogućava transparentnost lanaca snabdevanja i prikupljanje obaveštajnih podataka o zloupotrebama na tržištu rada. Protiv organizacija za koje se utvrdi da ne poštuju propise izriču se izvršne mere i šalju se poruke njihovim krajnjim korisnicima kako bi se podigla njihova svest, što bi potencijalno dovelo do gubitka posla (strategija „imenuj i osramoti").

U Ukrajini su nadležni organi počeli da blokiraju onlajn kanale na Telegramu koji šire informacije o seksualnoj eksploataciji.

## 3.2. Istraga slučajeva trgovine ljudima posredstvom IKT

Ovaj odeljak istražuje strategije i dobre prakse koje su osmislile države ugovornice kako bi povećale efikasnost istraga o trgovini ljudima posredstvom IKT (takve strategije i dobre prakse treba čitati zajedno sa strategijama koje se odnose na identifikaciju slučajeva o kojima je bilo reči iznad jer identifikacija i istraga mogu da budu usko povezane).

Nekoliko država je istaklo značaj **stalnog organizovanja obuka i razvojnih aktivnosti zasnovanih na najboljim lokalnim i globalnim praksama** za službenike za sprovođenje zakona. Uspostavljanje i obuka specijalizovanih jedinica za borbu protiv trgovine ljudima posredstvom IKT pominje se kao važna strategija. Uopšteno govoreći, mnoge države ugovornice smatraju da je **ulaganje u ljudski kapital** jednako ključno kao ulaganje u tehnološku opremu. Među specijalizovanim profilima koje su države identifikovale kao ključne za efikasno istraživanje trgovine ljudima posredstvom IKT, postoje službenici specijalizovani za „nove tehnologije", „operativni kriminalistički analitičar", „tajne istrage" i „istražitelji podataka iz otvorenih izvora – OSINT" (oznake su one navedene u francuskoj prijavi, ali druge države su ukazale

na slične profile). Kao što su grčki nadležni organi primetili, treba obezbediti obuku ne samo o tome kako se koriste tehnološki alati, već i o „njihovom etičkom korišćenju u pogledu poštovanja ljudskih prava i zaštite podataka" (više o obuci navedeno je u sledećem poglavlju).

Način na koji se obuka trenutno sprovodi razlikuje se od države do države. Jedan model je da se nacionalnim centrima za visokotehnološki kriminal, tamo gde su uspostavljeni, poveri zadatak razvoja alata i tehnika, i sticanja povezanih znanja, a zatim i zadatak širenja ovog znanja među policijskim jedinicama i/ili nuđenja pomoći integracijom drugih specijalizovanih jedinica, npr. jedinice za borbu protiv trgovine ljudima. Jasno je da je znanje o „naprednim istragama i analizi računarske tehnologije, uključujući bezbednost tragova i dokaza sa digitalnih uređaja, IKT sistema i od pružalaca internet usluga" ključna prednost (norveška prijava). Nekoliko država (ali ne sve) navelo je da imaju posebnu jedinicu koja se bavi kriminalom sa velikom tehnološkom komponentom, npr. jedinice/centre za sajber kriminal ili jedinice za visokotehnološki kriminal. Druge policijske jedinice, npr. specijalizovane jedinice za borbu protiv trgovine ljudima, mogu da traže pomoć od takvih jedinica.

Nekoliko država je primetilo značaj uključivanja specijalizovanih istražnih službenika sa „**digitalnim znanjem**" u istrage slučajeva trgovine ljudima. Takvi službenici se mogu angažovati da traže tragove trgovine ljudima na internetu. Jedan operativni model koji su predložili francuski nadležni organi bi podrazumevao prisustvo osoblja posebno obučenog za sprovođenje istraga na internetu i društvenim mrežama koje je integrisano u svaku jedinicu specijalizovanu za borbu protiv trgovine ljudima. Ono što je najvažnije, ovo osoblje bi moglo biti iz redova policijskih službenika sa policijskim ovlašćenjima ili ostalih policijskih službenika, npr. formiranjem grupa za tehničku podršku za „tradicionalne" istražitelje. Ova ideja se **udaljava od tradicionalnog policijskog modela** zasnovanog na policajcima pod zakletvom i usvaja princip – koje već primenjuju neke policijske uprave – da službenici koji nisu pod zakletvom imaju više tehničku ulogu (npr. analitičari).

Pored organizovanja obuke za službenike, bugarski nadležni organi su istakli značaj angažovanja IT stručnjaka u istragama trgovine ljudima, kao i poboljšane saradnje sa privatnim sektorom. Ovo su ponovili i kiparski nadležni organi koji su kao potencijalnu dobru praksu naveli formiranje timova istražitelja i analitičara specijalizovanih za trgovinu ljudima i visokotehnološki kriminal. Vrednost **međuagencijskog istražnog rada** uz učešće i saradnju širokog spektra specijalizovanog osoblja takođe je naglašena u prijavi Švajcarske u kojoj su, na primer, uspostavljeni zajednički timovi i ovaj model bi se mogao proširiti na trgovinu ljudima posredstvom IKT.

Nemački nadležni organi su ukazali na značaj poboljšanja **razmene znanja** među institucijama i **jačanja IKT veština** među policijskim službenicima. Prema španskim nadležnim organima, ključno je i „povećati svest o internet kriminalu" i „uključiti stručnjake za tehnološki kriminal u istrage trgovine ljudima od samog početka". Nekoliko država je navelo da treba organizovati i/ili ojačati obuke o tome kako da se nadgledaju i koordiniraju istrage trgovine ljudima sa velikom tehnološkom komponentom, jer elektronski dokazi postaju sve značajniji u slučajevima trgovine ljudima.

Postoji opšta saglasnost o **značaju nabavke i pristupa specijalizovanom softveru** za poboljšanje istraga o trgovini ljudima posredstvom IKT. U Holandiji, nadležni organi su kreirali alat za skeniranje mreže za prikupljanje i sistematizaciju velikih količina podataka. Holandski organi za sprovođenje zakona trenutno testiraju alat na konkretnim slučajevima trgovine ljudima kako bi izgradili pravosudni okvir. Prema holandskim nadležnim organima, sistem za skeniranje mreže „se fokusira na reklame sa rizikom od seksualne eksploatacije i trenutno je

u fazi testiranja"; nadležni organi takođe rade na utvrđivanju da li „postoji dovoljna pravna osnova i praktična upotrebljivost za njegovu upotrebu u formalnim istragama".

Slično tome, nekoliko drugih država, uključujući Estoniju, Republiku Moldaviju i Grčku, istaklo je **značaj velikih količina podataka, kao i poboljšanje sposobnosti za obradu velikih količina podataka**. Razvijanje ili nabavka alata koji mogu automatski da preuzimaju veb lokacije i druge vrste elektronskih informacija smatra se ključnim u vođenju istraga. Na primer, Biro litvanske kriminalističke policije je 2020. godine nabavio licencu za softver za prikupljanje informacija iz onlajn izvora i licencu za specijalizovani softver za analizu takvih informacija. Međutim, nije važna samo sposobnost prikupljanja podataka. Najvažnije je da takvi alati takođe moraju da budu u stanju da **čuvaju takve informacije na bezbedan način** kako bi se mogle *pouzdano* koristiti „kao dokaz na sudu ili kao obaveštajne informacije kako bi se izgradio slučaj" (prijava Švedske).

Druge dve vrste alata smatraju se ključnim za sprovođenje delotvornih istraga u slučajevima trgovine ljudima posredstvom IKT. Prvo, alati za preuzimanje informacija sa mobilnih telefona kada šifra nije dostupna (prijava Švedske). Drugo, razvoj i uvođenje alata koji omogućavaju dešifrovanje razgovora preko aplikacija za ličnu komunikaciju. Švedski nadležni organi su istakli da bi takvi alati takođe trebalo da budu u stanju da dešifruju razgovore u realnom vremenu. U Austriji, Kriminalistička obaveštajna služba razvija poseban softver za ispitivanje mobilnih telefona radi identifikacije žrtava trgovine ljudima.

Švajcarski nadležni organi su istakli potrebu za povećanjem **tajnih istraga** – kroz ulaganje u obuku specijalizovanih službenika. Slično tome, istakli su značaj policijskih službenika posebno obučenih u oblasti trgovine ljudima. Norveški nadležni organi smatraju tajne istrage „najefikasnijim istragama", posebno kada se kombinuju sa prikupljanjem velikih količina podataka iz OSINT veb pretraga, kao i podataka o transferima/tokovima novca. U Holandiji policija trenutno testira upotrebu „mamac profila" za identifikaciju trgovaca ljudima tokom njihovog pokušaja da regrutuju potencijalne žrtve. Slično tome, španski nadležni organi su istakli potrebu za prilagođavanjem nacionalnog zakonodavstva kako bi se u potpunosti iskoristile mogućnosti koje pružaju tajne istrage na internetu.

Britanski nadležni organi procenjuju da je **slojevitost informacija** ključna za istraživanje trgovine ljudima posredstvom IKT. Obogaćivanje obaveštajnih slika kombinacijom istraživanja podataka iz otvorenih izvora i sistema za sprovođenje zakona smatra se dobrom praksom. Takođe su predložili udaljavanje od jednostavnih lista indikatora. Na primer, primetili su da u kontekstu seksualne eksploatacije, istražitelji obično prate proces od tri koraka, za razliku od propisane liste indikatora, kako bi identifikovali visokorizične oglase na ASW. Prema takvom procesu, rizik se identifikuje tamo gde su ASW oglasi deo mreže, gde su prisutni indikatori prinude i kontrole i gde je autentičnost naloga za oglašavanje sumnjiva.

Nekoliko država je primetilo značaj unapređenja prekogranične saradnje i obezbeđivanja brze razmene podataka na operativnom nivou. Austrijski nadležni organi su kao primer dobre prakse naveli **međusobnu razmenu službenika** sa državama porekla žrtava. Uopšteno govoreći, ojačana međunarodna saradnja sa istražnim organima u državama porekla smatra se dobrom praksom.

Finski nadležni organi su istakli značaj sprovođenja **strateške analize** kako bi se prikupilo znanje o novonastalim trendovima i ažurirane informacije o *modusu operandi* (uključujući tehnologiju i veb lokacije koje koriste počinioci). Ovaj stav podržavaju i poljski nadležni organi. Prepoznato je da je stalno praćenje ove pojave teška i vremenski zahtevna aktivnost, koja

dodatno opterećuje (često) već preopterećene policijske resurse. Međutim, pristup ažuriranoj bazi znanja, uključujući tehnike regrutovanja koje koriste počinioci, smatra se veoma efikasnim sredstvom za prevenciju i borbu protiv trgovine ljudima. Ova vežba prikupljanja znanja treba da ima međunarodnu dimenziju – idealno uz određeni stepen međunarodne koordinacije. Na osnovu ovih zajedničkih dokaza, pojedinačne države tada mogu da pokrenu ciljane policijske operacije i zaključe sporazume o saradnji kad god je to relevantno.

Nekoliko država je primetilo da bi istrage mogle da budu **olakšane lakšim čuvanjem dokaza i pristupom na međunarodnom nivou**. Ovo se potencijalno prevodi u olakšane i pojednostavljene procedure za postupanje po upitima upućenim jedinicama nadležnim za čuvanje podataka u stranim državama (zahtevi za čuvanje podataka), kao i u olakšavanje zahteva za uzajamnu pravnu pomoć. Kako su, između ostalog, istakli poljski nadležni organi, „privatni sektor je taj koji najčešće poseduje informacije od značaja za organe za sprovođenje zakona (npr. podaci o pretplatnicima)" a „efikasno i brzo pribavljanje takvih podataka od strane policije je važno za pozitivno rešenje istrage".

## 3.3. Podsticanje međunarodne saradnje

Razmišljajući o svom iskustvu u postupanju u prekograničnim slučajevima trgovine ljudima posredstvom IKT, države su identifikovale sledeće „dobre principe" za podsticanje međunarodne saradnje:

- Korišćenje resursa dostupnih u agencijama kao što su Evropol i Evrodžast, kao i uspostavljanje zajedničkih istražnih timova.
- Uspostavljanje kontakta sa drugim stranama u **ranoj fazi** istrage. Ovo zahteva organizacione mere koje olakšavaju takve brze interakcije (npr. kroz jasnoću procedura i jasne kontaktne tačke).
- Razvijanje veoma dobrog **razumevanja pravnog konteksta i mogućnosti** saradnje sa predmetnom državom ili državama kako bi se izbegle blokade i obezbedila blagovremena saradnja.
- Održavanje **koordinacionih sastanaka** radi razmene informacija i dokaza što je brže moguće, kako bi se utvrdila zajednička strategija od *samog početka*; kako bi se olakšala realizacija zahteva za međunarodnu pravnu pomoć i kako bi se uklonile prepreke u vezi sa prihvatljivošću dokaza u predmetnoj državi.
- Razvijanje **zajedničkog razumevanja** standardizovanih pristupa i obezbeđivanje **transnacionalne interoperabilnosti** agencija za sprovođenje zakona kroz transnacionalne obuke.

Pored ovih opštih principa, postoji i niz konkretnih primera dobre prakse koje su identifikovale države ugovornice. Takve prakse se mogu grupisati u šest glavnih kategorija koje su opisane u nastavku.

**Zajednički istražni timovi**. Primer dobre prakse međunarodne pravne saradnje koju su prijavili bugarski nadležni organi je Zajednički istražni tim osnovan 2019. godine zajedno sa Francuskom – i uz pomoć Evrodžasta – koji se bavi borbom protiv trgovine ljudima, seksualnog zlostavljanja dece i trgovine trudnicama radi prodaje njihove dece. ZIT je sproveo veliki broj istražnih aktivnosti u Bugarskoj, Francuskoj, Nemačkoj i Grčkoj. Uopšteno govoreći, nekoliko prijava navodi zajedničke istražne timove kao primer dobre prakse. Kako su objasnili austrijski nadležni organi, oni omogućavaju „razmenu informacija kada su u pitanju transnacionalne istrage uz manje birokratije, kao i podelu nadležnosti između sudskih organa koji učestvuju".

**Saradnja između inspektorata rada**. Izvršna agencija bugarskog Opšteg inspektorata rada istakla je značaj koordinisanih inspekcija i istraga koje se zajednički sprovode u svim državama u složenim prekograničnim slučajevima koji uključuju potencijalnu radnu eksploataciju među radnicima upućenim na rad u inostranstvo[16]. Zajedničke akcije koje su sprovele inspekcije rada Bugarske i Francuske (projekat *Eurodétachement*) smatraju se primerima dobre prakse. Aktivnosti su uključivale zajedničke inspekcije u kompanijama za privremeno zapošljavanje koje šalju radnike u Francusku, kao i informativne sastanke za bugarske radnike koji su upućeni na rad u inostranstvo ili direktno zaposleni u Francuskoj (uglavnom u poljoprivredi). Održani su i onlajn sastanci radi razmene informacija i dobrih praksi o prekograničnim inspekcijama. Ovaj primer je naročito interesantan jer pokazuje **značaj nepolicijske saradnje** – koliko i policijske – u borbi protiv trgovine ljudima. Ipak, takvoj saradnji obično se posvećuje ograničena pažnja u izveštajima o politici. Države ugovornice bi možda želele da razmotre načine za poboljšanje saradnje između organa koji nisu policijski organi – naročito u kontekstu trgovine ljudima u svrhu radne eksploatacije.

**Strateška saradnja**. Nemački nadležni organi su istakli značaj strateške saradnje, na primer preko OA 7.1 projekta EMPACT koji se zasniva na Evropolu (*Evropska multidisciplinarna platforma protiv pretnji od kriminala*). Ovaj projekat se fokusira na trgovinu ljudima na internetu. U okviru projekta EMPACT, Holandija i Ujedinjeno Kraljevstvo razvijaju vizuelni pregled trgovine ljudima posredstvom IKT.

**Aktivnosti sajber patrola u koordinaciji EU/međunarodnih aktera**. Holandski i portugalski nadležni organi su naveli EMPACT dane zajedničkih akcija/koordinirane akcije sajber patrola na internetu/mračnoj mreži kao primer dobre prakse u međunarodnoj saradnji. Obaveštajni podaci se prvo prikupljaju u pojedinim državama, a zatim se prelazi na koordinisane akcije.

**Korišćenje mreže oficira za vezu**. Poljski i francuski nadležni organi su istakli značaj akreditovanih oficira za vezu za olakšavanje razmene informacija. Francuski nadležni organi su ukazali na slučaj u kojem je podrška rumunskih oficira za vezu sa sedištem u Francuskoj omogućila istovremeno hapšenje u obe države. Na ovaj način, nadležni organi su mogli da sruše čitavu transnacionalnu kriminalnu mrežu, uključujući i njenog šefa koji je upravljao operacijama u Francuskoj dok je živeo u Rumuniji. Norveški nadležni organi su istakli prednost postojanja kontaktne tačke na Filipinima za razmenu informacija o aktuelnim slučajevima, čime se izbegavaju dupliranja u istragama i sukobi. Preko kontaktne tačke, norveški i filipinski nadležni organi su bili u mogućnosti da razmene iskustva, trendove i studije, uključujući i u pogledu trgovine ljudima posredstvom interneta.

## 3.4. Identifikacija žrtava i pomoć žrtvama

Ovaj odeljak se fokusira na načine kako države ugovornice koriste tehnološke alate u vezi sa: (a) identifikacijom žrtava; (b) pomoći i (c) širenjem informacija među ugroženim zajednicama.

### 3.4.1. Tehnološki alati za identifikaciju žrtava trgovine ljudima

Čini se da se tehnološki alati zasnovani na **prepoznavanju lica** često koriste u slučajevima seksualne eksploatacije dece (CSE), npr. za unakrsno proveravanje fotografija u postojećim međunarodnim bazama podataka, kao što je baza podataka NCMEC (Nacionalni centar za

16 Prema Direktivi 96/71/EZ i Informacionom sistemu unutrašnjeg tržišta (IMI).

nestalu i eksploatisanu decu, SAD) ili Interpolova ICSE[17]. Međutim, čini se da je upotreba takvih alata ograničenija izvan oblasti seksualne eksploatacije dece. Finski nadležni organi su naveli da sprovode testove alata za prepoznavanje lica kako bi identifikovali žrtve seksualne eksploatacije na internetu, posebno u kontekstu veb kamera. Takođe su predložili da se upotreba takvih alata može proširiti kako bi obuhvatila širi spektar situacija trgovine ljudima. Letonski nadležni organi su spomenuli upotrebu specijalizovanog softvera za prepoznavanje fotografija (PhotoDNK, Clear View) u pojedinačnim slučajevima. U Mađarskoj se tokom istrage može koristiti ciljana upotreba alata za prepoznavanje lica kako bi se identifikovale potencijalne žrtve. Među nekoliko država koje su navele da koriste tehnološke alate za identifikaciju žrtava trgovine ljudima pomoću velikih količina podataka, Nemačka je nedavno uvela alat za skeniranje veb lokacija koje sadrže oglase za seksualne usluge kako bi se pomoglo u identifikaciji žrtava trgovine ljudima. Austrijski istražitelji imaju pristup **sistemima za skeniranje mreže radi prikupljanja podataka** i (pod određenim uslovima) alatima za prepoznavanje lica. U Ujedinjenom Kraljevstvu, nadležni organi koriste alate za „struganje" na internetu za prikupljanje i analizu podataka sa veb lokacija za usluge za odrasle (ASW) kako bi se pomoglo u identifikaciji žrtava trgovine ljudima.

Što se tiče upotrebe **indikatora trgovine ljudima** (**„znaka upozorenja"**), nekoliko država je prijavilo da se *oslanja* na indikatore za potrebe identifikacije slučajeva trgovine ljudima; međutim, ovo su „opšti" indikatori trgovine ljudima i nisu specifični za trgovinu ljudima posredstvom IKT. Ovo nije iznenađujuće, budući da je razvoj indikatora („znakova upozorenja") specifičnih za trgovinu ljudima posredstvom IKT daleko od jednostavnog – kao što je detaljno razmotreno u Poglavlju 2. Norveški nadležni organi su naveli da, iako „imaju skup indikatora za identifikaciju žrtava trgovine ljudima", predmetni skup treba revidirati i proširiti kako bi bio prikladan „okruženju istrage kriminala u vezi sa IKT". Ovaj posao trenutno obavlja Norveška nacionalna ekspertska grupa za borbu protiv trgovine ljudima.

Britanski nadležni organi su izvestili da koriste listu indikatora za pomoć pri **identifikaciji žrtava na ASW**. Njihovo iskustvo u korišćenju ovakvih indikatora zajedno sa alatom za „struganje" interneta je posebno značajno. Prema dostavljenim dokazima, iako ovi indikatori mogu da pruže određenu pomoć, oni „treba da se koriste u kombinaciji sa analizom mreže i procenom autentičnosti naloga kako bi se obezbedila najbolja praksa". Ovo ukazuje na poteškoće u automatizaciji identifikacije žrtava – i na granice preteranog oslanjanja na unapred utvrđenu listu indikatora. Štaviše, britansko iskustvo pokazuje značaj kombinovanja različitih metoda, uključujući **analizu društvenih mreža** i **ljudsku procenu** dokaza. Ponovo se jasno primećuje ključna uloga analitičara/istražitelja – kao i potreba da se oni delotvorno obuče. Alati mogu biti veoma dragoceni u vršenju redukcije podataka i rukovanju velikim količinama informacija; međutim, potrebno je da ih koriste dobro obučeni operateri sa znanjem o specifičnoj temi/problemu (npr. trgovina ljudima).

Korišćenje veštačke inteligencije i tehnoloških alata za identifikaciju žrtava ima svoje izazove, uključujući **etička pitanja** i potencijal za diskriminaciju (npr. profilisanje zasnovano na diskriminatornim kriterijumima; videti i diskusiju u Poglavlju 6). Švedska policijska uprava je izrazila zabrinutost u vezi sa „upotrebom AI tehnologije za identifikaciju žrtava trgovine ljudima".

Na kraju, Kancelarija grčkog nacionalnog izvestioca i Laboratorija za prava Univerziteta u Notingemu uvode projekat koji koristi satelitske podatke i metode daljinskog otkrivanja za praćenje radnih uslova i mobilnosti radnika migranata u poljoprivredi. Grčki izvestilac je u

17 Među tehnološkim alatima koje države koriste u borbi protiv seksualne eksploatacije dece (CSE), nalaze se „Gridcop" i „IcacCops". Islandska policija koristi „Griffeye" za obradu, sortiranje i analizu fotografija i video zapisa zaplenjenih tokom istraga CSE i vrši unakrsne provere ovih fotografija sa međunarodnim bazama podataka.

procesu razvoja daljih tehnoloških aplikacija za identifikaciju žrtava trgovine ljudima u sektoru poljoprivrede i učinio je razvoj novih tehnoloških aplikacija ključnom komponentom Nacionalnog akcionog plana 2019–2023.

### 3.4.2. Inicijative zasnovane na tehnologiji za pomoć žrtvama i širenje informacija među ugroženim zajednicama

Ovaj odeljak predstavlja pregled inicijativa zasnovanih na tehnologiji koje su osmišljene da pomognu žrtvama i šire informacije među ugroženim zajednicama. Imajte na umu da su inicijative o kojima se govori u nastavku identifikovane od strane država ugovornica.

**Mehanizmi za prijavljivanje na internetu i telefonske linije za pomoć**. Nekoliko država ima uspostavljene mehanizme za anonimno prijavljivanje viktimizacije, kao i za primanje početne pomoći putem telefonske linije za pomoć. Neke telefonske linije za pomoć nude 24-časovnu podršku i mogu da upute žrtve na socijalne službe, kao i da objasne procedure i prava. U Holandiji postoji nekoliko organizacija koje nude **digitalnu pomoć putem funkcije ćaskanja** („Fier" i „Slachtofferhulp Nederland" su dve od tih organizacija). Takve organizacije nude početno savetovanje, pomoć i mogućnost anonimnog prijavljivanja seksualne eksploatacije. Funkcija ćaskanja nije samo reaktivna, već služi i za proaktivno uspostavljanje kontakta sa pojedincima u riziku. Holandsko ministarstvo pravde i bezbednosti trenutno istražuje kako se ovaj alat može dalje razvijati u saradnji sa relevantnim zainteresovanim stranama. U Francuskoj, Ministarstvo unutrašnjih poslova vodi platformu za prijavljivanje seksualnog i rodno zasnovanog nasilja (PVSS). Žrtve mogu da stupe u kontakt sa zvaničnikom putem **sistema za razmenu poruka/onlajn ćaskanja**, da podnesu prijavu i dobiju prvu pomoć.

**Zvanični onlajn materijali**. Informativni materijali koje pripremaju nadležni organi često se postavljaju na zvanične veb lokacije. U Austriji, na primer, informacije za žrtve trgovine ljudima koje priprema Savezno ministarstvo unutrašnjih poslova, kao i nevladine organizacije, dostupne su na nekoliko jezika na različitim onlajn platformama i društvenim medijima. Na veb lokaciji Federalnog ministarstva pravde, žrtve trgovine ljudima mogu pristupiti materijalima na 16 jezika o njihovim pravima na psiho-socijalnu i pravnu podršku. U Poljskoj, Ministarstvo unutrašnjih poslova i uprave i Ministarstvo spoljnih poslova vodili su onlajn informativnu kampanju putem veb lokacije „e-konsulat" sa banerom koji prikazuje informacije o trgovini ljudima na nekoliko jezika i preusmerava onlajn posetioce na Konsultantski i interventni centar za žrtve trgovine ljudima (KCIK). Pored zvaničnih kanala, nekoliko država je istaklo važnu ulogu koju imaju NVO u širenju informacija putem svojih veb lokacija, kao i zvaničnih naloga na društvenim medijima kao što su Facebook, Instagram i YouTube.

**Onlajn alati i aplikacije**. Bugarska nacionalna komisija za borbu protiv trgovine ljudima pokrenula je onlajn alat za prevenciju u okviru godišnje kampanje za prevenciju trgovine ljudima u svrhu radne eksploatacije. Internet alat je kreiran u saradnji sa češkom NVO i bio je namenjen Bugarima koji traže posao u Češkoj. Alat je pružio informacije o uslovima rada i rizicima od kršenja prava radnika. Kako je primetila Bugarska komisija, „efikasnost ovog pristupa je naglašena činjenicom da je ubrzo nakon što je alat počeo da funkcioniše, napravljen lažni alat sa ciljem da privuče potencijalne žrtve radne eksploatacije". U Litvaniji je nedavno razvijena aplikacija pod nazivom „Raktas" (dostupna u prodavnici Google Play) kako bi se podigla svest Litvanaca koji žive i rade u inostranstvu o ranim znacima trgovine ljudima. Kao budući razvoj, aplikacija će uključivati mogućnost za ćaskanje preko koje će litvanska žrtva ili potencijalna žrtva trgovine ljudima moći da kontaktiraju litvansku NVO u realnom vremenu i zatraže podršku. Portugalska Uprava za uslove rada razvila je aplikaciju „ACT ", Agir Contra o Tráfico. Nadležni organi Estonije prijavljuju upotrebu masovnog obaveštavanja putem

SMS/tekstualnih poruka kao deo kampanje protiv seksualne eksploatacije. Španija je 2017. godine pokrenula mobilnu aplikaciju „Chicas Nuevas 24 horas: Happy" kako bi omogućila mladim ljudima da otkriju, kroz video igru, putovanje devojke (Happy) od njenog rodnog grada u Nigeriji do iskustva seksualne eksploatacije u Španiji.

**Kampanje za podizanje svesti na internetu**. U Bugarskoj, Nacionalna komisija za borbu protiv trgovine ljudima (NCCTHB) svake godine sprovodi tri nacionalne kampanje za prevenciju i informisanje sa nizom događaja koji se fokusiraju na prevenciju trgovine ljudima u svrhu prinudnog rada i seksualne eksploatacije. Materijali se takođe distribuiraju putem interneta. Tokom kampanje oktobar/novembar 2018. godine, kampanja je došla do preko dva miliona bugarskih aktivnih korisnika na mrežama Facebook i Instagram. Generalno, aktivnosti NCCTHB i povezani onlajn alati za prevenciju redovno se objavljuju na društvenim medijima. Takve objave imaju oko 100.000 pregleda godišnje. Pored toga, diskusije o IKT, internetu, društvenim medijima i uticaju novih tehnologija na trgovinu ljudima, kao i o njihovoj upotrebi za regrutovanje i eksploataciju žrtava, uključeni su u različite aktivnosti za podizanje svesti na nacionalnom i lokalnom nivou, usmerene pre svega na mlade ljude i studente. Izvršna agencija Generalne inspekcije rada organizuje i učestvuje u informativnim kampanjama o rizicima u vezi sa radom u inostranstvu; takođe upravlja i telefonskom linijom za savetovanje i prijavljivanje koja je takođe otvorena za bugarske državljane koji rade u inostranstvu.

U Irskoj, aktuelna kampanja pod nazivom „Blue Blindfold" koju vodi Ministarstvo pravde redovno širi informacije među ugroženim zajednicama putem namenske veb lokacije, štampanih medija i kampanja na društvenim mrežama.

U Nemačkoj, Savezno ministarstvo za ekonomsku saradnju i razvoj razvilo je projekte sa državama partnerima za prevenciju i borbu protiv trgovine ljudima. Na primer, u okviru projekta „Sprečavanje trgovine ljudima na Zapadnom Balkanu i podrška žrtvama", Regionalna inicijativa za migracije, azil i izbeglice (MARRI) izradila je smernice i informativne materijale za kampanje za podizanje svesti javnosti i učinila ih je dostupnim na internetu. Imajući u vidu da se internet sve više koristi za regrutovanje žrtava trgovine ljudima, jedan od alata se fokusirao na pretnje kojima su deca izložena na internetu[18].

U Rumuniji, Nacionalna agencija za borbu protiv trgovine ljudima (NAATIP) vodi kampanje na mrežama Facebook, Youtube, a od 2020. godine i na mrežama Instagram, Twitter i LinkedIn. Objave na mreži Facebook stigle su do 2,5 miliona korisnika tokom 2020. godine (+300% u odnosu na prethodnu godinu). Primeri kampanja uključuju:

(a) Svakodnevno objavljivanje preventivnih poruka na društvenim mrežama o borbi protiv trgovine ljudima i različitim vidovima eksploatacije (seksualna eksploatacija, radna eksploatacija i prinudno prosjačenje);
(b) Onlajn kampanja pod nazivom „The perfect Job – one way illusion" (Savršen posao – iluzija u jednom smeru) u partnerstvu sa OLX iz Rumunije (veb servis koji objavljuje objave) sa ciljem prevencije trgovine ljudima kroz povećanje svesti među ljudima koji traže posao preko onlajn platformi;
(c) Angažovanje dva poznata rumunska YouTube vlogera koji zajedno imaju publiku od 1,3 miliona pratilaca kako bi se povećala vidljivost i efikasnost NAATIP poruka protiv trgovine ljudima. Vlogeri su snimili dva video snimka o trgovini ljudima koji su u prvim satima emitovanja postigli oko 100.000 pregleda na mreži YouTube.

18 „Minors at risk of cyber-trafficking" (toolboxes.marri-rc.org.mk/tips/minors-at-risk-of-cyber-trafficking).

Ukratko, važno je napomenuti da, kako su istakli bugarski nadležni organi, efikasna kampanja zahteva „mnogo pripremnog rada" kako bi se u potpunosti razumelo kome je namenjena i kako bi se adekvatno razvila njena poruka. Na kraju krajeva, to zahteva ulaganja. Dobra praksa je rad sa privatnim kompanijama na izradi **društvenog oglašavanja**. Ovo se može postići, na primer, putem publikacija koje sponzorišu kanali društvenih medija, kao što su Facebook i Instagram (platforma bi mogla da obezbedi besplatan prostor, kao i stručnost u dizajniranju kampanje/poruke). Jasno je da ciljane i dobro razvijene onlajn kampanje mogu da predstavljaju koristan alat. Primer kampanje koju je vodila bugarska Nacionalna komisija za borbu protiv trgovine ljudima mnogo govori. U okviru kampanje – osmišljene da podigne svest o trgovini ljudima u svrhu radne eksploatacije – napravljen je i distribuiran vizuelni prikaz primera obmanjujuće ponude za posao. Korisnici su pogrešno protumačili ponudu za posao kao pravu i počeli da zovu kancelariju Nacionalne komisije, raspitujući se o poslu (za više detalja o kampanji videti odeljak 1.1.2). Ovaj primer pokazuje potencijalni domet/uticaj obmanjujućih oglasa za posao, ali je takođe ponudio Komisiji „dobru priliku da informiše tražioce posla koji su spremni da prihvate rizične ponude".

Međutim, kako su upozorili bugarski nadležni organi, postoji **rizik od preteranog oslanjanja na onlajn kampanje** pri pokušaju da se dopre do potencijalnih žrtava. U nekim slučajevima, takve žrtve dolaze iz „ranjivih zajednica" koje karakterišu nizak nivo obrazovanja i ograničeno poznavanje tehnoloških alata i resursa. U tim okolnostima, pristup zasnovan na direktnom (ličnom) pristupu (i dalje) ima važnu ulogu kao preventivna strategija.

Na kraju, inspiracija za inicijative može poteći iz projekata koji se bave pitanjima sličnim trgovini ljudima posredstvom interneta i tehnologije. U Finskoj, na primer, NVO Women's Line pokrenula je projekat pod nazivom *Turv@verkko*, koji ima za cilj sprečavanje sajber nasilja nad ženama i devojčicama i pružanje pomoći žrtvama. Slično tome, Youth Exit i *Sua varten* usmereni su na mlade korisnike interneta kako bi sprečili seksualno uznemiravanje na internetu. Iako nisu direktno povezane sa trgovinom ljudima, takve inicijative mogu da ponude korisne naznake za razvoj projekata namenjenih žrtvama trgovine ljudima.

## 3.5. Dokazi prikupljeni od NVO

NVO su izvestile o brojnim strategijama za unapređenje pomoći u otkrivanju žrtava i podizanje svesti u vezi sa trgovinom ljudima posredstvom interneta i tehnologije.

La Strada International, KOK (Nemačka), Astrée (Švajcarska) i La Strada Moldova naglasili su značaj **odgovarajućih i ažuriranih informacija** kojima žrtve trgovine ljudima i pojedinci podložni eksploataciji i zlostavljanju mogu lako da pristupe na internetu. Ovo bi trebalo da uključuje informacije o organizacijama za podršku i njihovim telefonskim linijama za pomoć. Takve onlajn platforme takođe treba da **omoguće samoidentifikaciju** žrtava. La Strada International je istakla da relevantne informacije do kojih dođu NVO treba podeliti sa organima za sprovođenje zakona – nakon što se dobije saglasnost relevantnih lica. Predviđene su inicijative za povećanje samoprijavljivanja takođe i u vezi sa radnom eksploatacijom, npr. u formi onlajn platformi i aplikacija putem kojih pojedinci mogu anonimno da prijave zloupotrebe na licu mesta (dokazi koje je pružila Sustainable Rescue Foundation iz Holandije).

Dostupnost onlajn informacija i mehanizama za samoidentifikaciju treba da se kombinuje sa **kampanjama za podizanje svesti**. La Strada International smatra da su dve vrste kampanja posebno važne: (a) one koje su direktno usmerene na potencijalne žrtve i pojedince koji su u riziku od eksploatacije i zlostavljanja; i (b) one koje su usmerene na zainteresovane

strane da prepoznaju rizike od trgovine ljudima posredstvom tehnologijom i da ih prijave. Organizacije Different and Equal (Albanija) i KOK (Nemačka) istakle su značaj edukacije korisnika IKT o rizicima vezanim za tehnologiju. One su predložile vođenje širih **kampanja za podizanje svesti o tome kako trgovci ljudima mogu da koriste tehnologiju** i o rizicima sa kojima se pojedinci mogu suočiti (naročito mlađi korisnici). Naglasak treba staviti na regrutovanje, posebno na to kako bi potencijalna eksploatatorska situacija mogla da počne (tj. kako trgovci ljudima uspostavljaju prve kontakte). Kompanije koje pružaju onlajn i IKT usluge treba da učestvuju u ovim naporima. Migrant Rights Centre Ireland je dalje napomenuo da kompanije za društvene medije treba da rade na odvraćanju.

Osim toga, nekoliko NVO, uključujući La Strada International i Sustainable Rescue Foundation, podvuklo je značaj povećanja i unapređenja **razmene podataka** među relevantnim zainteresovanim stranama. Ove razmene bi trebalo da obuhvataju najnovija saznanja o rizicima vezanim za tehnologiju.

NVO su istakle značaj razvoja znanja o rizicima vezanim za IKT i uopšteno o trgovini ljudima posredstvom tehnologije, takođe među organizacijama koje pomažu žrtvama, uključujući one koje pružaju savetodavne usluge. Pošto je **očuvanje elektronskih dokaza** ključno za razvoj jakih istraga, od ključnog je značaja da pripadnici prve linije borbe iz redova savetnika i NVO budu upoznati sa strategijama za očuvanje digitalnih dokaza (npr. čuvanjem istorije ćaskanja). Nuđenje sveobuhvatne obuke o bezbednosti i sledljivosti podataka na internetu za savetnike i NVO smatra se ključnim.

Organizacija FIZ (Švajcarska) je primetila da IKT, uključujući društvene medije i onlajn informacije, mogu da pomognu NVO da uspostave kontakte sa potencijalnim žrtvama i prikupe dodatne informacije o okolnostima eksploatacije. Ako budu upozorene na sumnjivu situaciju, NVO mogu da **iskoriste informacije dostupne na internetu za uspostavljanje kontakta sa potencijalnom žrtvom**.

Migrant Rights Centre Ireland i Astrée (Švajcarska) predložili su osnivanje namenskih jedinica za istraživanje digitalnog kriminala koje bi bile stručne za borbu protiv trgovine ljudima posredstvom tehnologije. Organizacija Praksis (Grčka) je pozvala na jačanje stručnosti organa za sprovođenje zakona u pogledu IKT i pratećih rizika. Štaviše, ona je pozvala na pojačanu saradnju i razmenu između nadležnih organa i privatnih kompanija.

Dokazi prikupljeni od NVO potvrđuju da korišćenje „**znakova upozorenja**" u slučajevima trgovine ljudima posredstvom tehnologije nije rasprostranjeno. NVO prijavljuju korišćenje standardnih indikatora, ali pozivaju na **reviziju takvih indikatora** kako bi se razmotrile specifičnosti IKT posredstvom tehnologije – naročito u vezi sa regrutovanjem i eksploatacijom posredstvom IKT. Organizacija KOK (Nemačka) je sugerisala da praćenje veb lokacija na kojima klijenti razmenjuju iskustva o kupovini seksualnih usluga može pružiti nagoveštaje o prisilnoj prostituciji/trgovini ljudima. Pregled „znakova upozorenja" mogao bi da uključuje indikatore koji su primenjivi na takve veb lokacije.

### 3.5.1. Fokus na inicijative koje se zasnivaju na tehnologiji

La Strada International smatra da njeni članovi i druge NVO „sve više" koriste tehnologiju. Međutim, iako su se „tehnički resursi i mogućnosti enormno povećali", stepen u kojem NVO koriste tehnologiju ostaje „ograničen". Kako navodi La Strada International, tehnologija se uglavnom koristi za registraciju podataka, a zatim i njihovu analizu, kao i za praćenje aktivnosti pružanja pomoći. NVO sve više koriste tehnologiju, uključujući društvene medije, za

vođenje kampanja (npr. kampanje za podizanje svesti; videti u nastavku) i za pružanje informacija, kao i za „stupanje u kontakt sa grupama u riziku ili za angažovanje sa zajednicama na internetu" (prijava La Strada International). U okviru ove studije, od NVO je traženo da navedu primere inicijativa zasnovanih na tehnologiji za poboljšanje otkrivanja trgovine ljudima posredstvom interneta i tehnologije, identifikaciju žrtava i prevenciju budućih slučajeva. U nastavku je dat kratak pregled ovakvih inicijativa na osnovu dokaza koje su pružile NVO.

### *Samoprijavljivanje putem interneta i kontakt sa potencijalnim žrtvama*

- Organizacija La Strada Moldova je ukazala na onlajn mehanizme za decu pomoću kojih mogu sami da prijave probleme bezbednosti na internetu (www.siguronline.md). To uključuje neprijatne situacije sa kojima se dete moglo suočiti na internetu. Dete tada stupa u kontakt sa specijalizovanim savetnikom i, ako se otkriju dokazi o seksualnom zlostavljanju ili eksploataciji na internetu, slučaj se prijavljuje policiji.
- U Švajcarskoj, organizacija Astrée je primetila sve veći broj žrtava koje se same prijavljuju za njene usluge, kao i sve veći broj potencijalnih žrtava koje su uputili prijatelji ili klijenti zahvaljujući prisustvu organizacije na internetu. Astrée takođe nudi onlajn obrazac za uspostavljanje kontakta i traženje pomoći. Dalje, FIZ je ukazao na uspešnu upotrebu platformi društvenih medija za uspostavljanje kontakta sa potencijalnim žrtvama trgovine ljudima, ako je poznato ime osobe. Veb lokacija „Nacionalne platforme protiv trgovine ljudima" iz Švajcarske sadrži veze do brojnih organizacija koje mogu da pruže pomoć.
- Organizacija Fair Work (Holandija) koristi društvene medije da dopre do migrantskih zajednica kako bi identifikovala žrtve trgovine ljudima ili eksploatacione situacije. Fair Work prvo identifikuje Facebook stranice koje su relevantne za određenu ciljnu grupu, a zatim deli informacije preko takvih stranica. Ona kreira anonimne lične naloge, koje vode volonteri, a koji se koriste za prevenciju. Kako radnici migranti često koriste društvene medije za pronalaženje informacija, ove tehnike se mogu iskoristiti da pomognu pojedincima u riziku „da postanu manje izolovani i više osnaženi" i da smanje rizike od trgovine ljudima (prijava La Strada International). Međutim, ovo nije uvek lak zadatak, jer „žrtvama nije uvek lako da znaju gde da traže odgovarajuće informacije, kojim informacijama mogu da veruju; kome da se obrate i da nađu ko im najbolje može pomoći, naročito ako slabo poznaju državu i svoja prava u toj državi".
- Organizacija La Strada International je prijavila da su neki od njenih članova razvili konsultantske servise za ćaskanje na internetu za traženje saveta i prijavu eksploatacije i zlostavljanja – pored telefonskih linija za pomoć.
- La Strada International je takođe prijavila da njeni članovi obično koriste onlajn platforme, kao što su Facebook, Instagram, LinkedIn, i sopstvene veb lokacije, kako bi informisali javnost o svom radu. Slično tome, organizacija KOK (Nemačka) je prijavila da njeni članovi koriste veb lokacije, Facebook i WhatsApp za širenje informacija i uspostavljanje kanala komunikacije za potencijalne žrtve. Ono što je najvažnije, jedna organizacija klijentima nudi WhatsApp broj za prijavu znakova potencijalne eksploatacije među seksualnim radnicima.

### *Mobilne aplikacije za podizanje svesti i traženje pomoći/informacija*

- Organizacija La Strada u Češkoj Republici bila je uključena u kreiranje SAFE, aplikacije koju je razvio IOM Slovačka u obliku interaktivne igre dizajnirane da spreči trgovinu ljudima. Igrajući igru, korisnici procenjuju svoj rizik u pogledu trgovine ljudima; aplikacija takođe sadrži informacije o bezbednom putovanju, radu u inostranstvu i korisnim kontaktima u hitnim slučajevima. Astra (Srbija) je razvila BAN Human Trafficking, aplikaciju čiji cilj je da mlade ljude upozna sa situacijama koje potencijalno dovode do eksploatacije i da pruži savete za uočavanje takvih situacija. Plan im je da nadograde aplikaciju funkcijom za prijavu eksploatatorskih praksi.

- Organizacija La Strada International je primetila razvoj aplikacija od strane NVO za prijavu eksploatacije i zlostavljanja, kao što je, na primer, aplikacija koju je razvila Unseen (Ujedinjeno Kraljevstvo). U Albaniji, organizacija Different and Equal učestvuje u razvoju različitih mobilnih aplikacija (npr. *„#raporto #shpeto"*) koje su namenjene da pomognu žrtvama trgovine ljudima i rodno zasnovanog nasilja (*„#GjejZa"*).
- Organizacija La Strada International je dalje primetila razvoj aplikacija za podršku ranjivim grupama, na primer, za pružanje pristupa informacijama ili informacija o radnim pravima u državi odredišta. Jedan od primera je aplikacija Workenn: igra za integraciju migranata na tržište rada, proizvedena u okviru Sirius projekta za pomoć migrantima koji traže posao. Kao jedan od primera izvan Evrope možemo pomenuti Apprise Audit – platformu koju su razvili klub Mekong i Univerzitetski institut UN u Makau, koja omogućava bezbedne i poverljive razgovore sa radnicima na njihovom maternjem jeziku.

### *Onlajn kampanje za podizanje svesti*

- Organizacija La Strada Moldova sprovela je kampanju za podizanje svesti tokom „Dana bezbednijeg interneta 2019. godine" sa ciljem podizanja svesti o seksualnoj iznudi među mladima. Ljudi su podstaknuti da prijavljuju slučajeve putem bezbednog onlajn mehanizma za prijavljivanje (www.siguronline.md). Kampanja je doprla do oko 70.000 onlajn korisnika. Ista organizacija testirala je strategije profilisanja kako bi usmerila svoje onlajn poruke odabirom starosne kategorije onlajn korisnika, njihovih interesovanja i profila.
- Organizacija Different and Equal (Albanija) organizovala je nekoliko kampanja za podizanje svesti na internetu koristeći društvene mreže i aplikacije (uključujući Facebook, Instagram, Twitter, veb lokaciju i YouTube) koje su bile naročito usmerene na sprečavanje trgovine ljudima, seksualnog zlostavljanja i porodičnog nasilja (kampanja je doprla do oko 15.000 korisnika). Kampanja je pokrenuta, u saradnji sa drugim NVO, tokom pandemije kovida-19.
- Organizacija Novi put (Bosna i Hercegovina) organizovala je nekoliko kampanja za podizanje svesti koje su bile fokusirane na korišćenje tehnologije u vezi sa trgovinom ljudima i seksualnom eksploatacijom dece.
- Astra (Srbija) organizovala je kampanje za podizanje svesti o najvažnijim načinima regrutovanja, uključujući ponude za posao na internetu i vrbovanje preko mreže Facebook i društvenih mreža, kao i o strategijama za kontrolu i eksploataciju žrtava (uključujući praćenje žrtava korišćenjem dostupnih opcija za praćenje lokacije u često korišćenim aplikacijama).

### *Ostale inicijative*

- Organizacija Astra (Srbija) je 2018. godine sprovela eksperiment „virtuelne devojčice" – napravila je profil petnaestogodišnje devojčice koja koristi internet. U roku od 24 sata, ovaj profil je primio preko 3.000 zahteva, uključujući ponude za posao i eksplicitne seksualne ponude od odraslih muškaraca (dokazi koje je dostavila La Strada International).
- Organizacija Different and Equal (Albanija) u okviru svog programa reintegracije organizuje obuku o korišćenju računara i tehnologije, koja uključuje tehnike zaštite podataka.
- La Strada International je prijavila neke javno-privatne inicijative u koje su uključene NVO, npr. projekat koji je pokrenuo Univerzitet u Amsterdamu sa velikim holandskim bankama u cilju identifikacije slučajeva trgovine ljudima. U okviru ove inicijative konsultovane su NVO sa sedištem u Holandiji, uključujući FairWork, CoMensha i La Strada International.

### *Pogled u budućnost i rešavanje najvažnijih pitanja*

Među NVO vlada opšta saglasnost da se više može učiniti kako bi se iskoristila tehnologija, naročito za širenje informacija, pristupanje i komunikaciju sa potencijalnim žrtvama – kao i za prijem saveta i izveštaja. Organizacija FIZ (Švajcarska) je predložila da se dalje razvijaju alati

za anonimno prijavljivanje nasilja i eksploatacije, i da se obezbede kontakti sa NVO koje nude usluge zaštite i savetovanja žrtava. Organizacija KOK (Nemačka) je ukazala na značaj daljeg razvoja vizuelnih materijala, npr. video zapisa, slika i aplikacija, koji će se koristiti tokom obuke, kao i za širenje na internetu, uključujući i među rizičnim zajednicama.

NVO su takođe otvorile neka **najvažnija pitanja** u vezi sa inicijativama i tehnološkim alatima. La Strada International je istakla da se tehnološki alati uglavnom izrađuju u okviru samostalnih projekata i da „često ne uključuju periode testiranja". Dakle, dostupni su nam ograničeni dokazi o njihovoj efikasnosti. Osim toga, kada više nema finansijske podrške za projekat, često ne postoji dugoročna finansijska strategija za promovisanje i korišćenje proizvedenih alata. Ovo je naročito problematično jer je za alate potrebno „kontinuirano ažuriranje i obučavanje".

Organizacija La Strada International je dalje primetila da inicijative „često nemaju dovoljno učešća NVO i drugih zainteresovanih strana koje bi trebalo da koriste alate u praksi i stoga treba da imaju izvestan osećaj vlasništva". Takođe je istakla „da je i dalje nejasno kakav je uticaj tehnologije na efikasno sprečavanje ili borbu protiv trgovine ljudima", što dovodi u pitanje da li „[su] nadzor i profilisanje na granicama, kao i na drugim lokacijama, zapravo doveli do identifikacije žrtava trgovine ljudima" i da li su lica identifikovana pomoću tehnologije tada dobila „pomoć i zaštitu". Organizacija poziva na **više evaluacije i procene uticaja** „svih razvijenih tehnoloških alata". „Da li su ovi – često skupi – alati služili potrebama zainteresovanih strana u borbi protiv trgovine ljudima i da li su alati u stvari testirani i dobro korišćeni, a ako nisu, zašto nisu?", pitala je a.

Ono što je najvažnije, NVO su naglasile da, sve u svemu, još uvek postoji ograničena dostupnost tehnoloških alata koje praktičari mogu da koriste. Da bi odgovarali potrebama NVO, **alati moraju biti „jeftini i laki za upotrebu".** Sustainable Resource Foundation je dalje upozorila da „alati stvaraju višak podataka za različite korisnike", pa je stoga važno da budu razvijeni imajući u vidu specifične potrebe i sveobuhvatnu strategiju kako bi se izbeglo dupliranje alata koji obavljaju (lake) funkcije, dok im nedostaju alati koji obavljaju više strateške, složenije funkcije.

## 3.6. Dokazi prikupljeni od tehnoloških kompanija

Facebook je izvestio o različitim oblicima **saradnje sa NVO** iz celog sveta u cilju kreiranja obrazovnih kampanja koje podižu svest o rizicima seksualne eksploatacije na internetu – posebno među mladim korisnicima – kao i o pravima potencijalnih žrtava trgovine ljudima i kućnog ropstva. Takve kampanje takođe pružaju informacije o telefonskim linijama za trgovinu ljudima koje nude pomoć i podršku. Primera radi, Facebook je naveo kampanju za podizanje svesti o trgovini radnicima/kućnom ropstvu pokrenutu u martu 2021. godine u partnerstvu sa organizacijom Stop the Traffik, koja je imala za cilj da pruži informacije domaćim i niskokvalifikovanim radnicima na Filipinima o njihovim pravima, o lokalnim smernicama za zapošljavanje u inostranstvu i o dostupnim telefonskim linijama za pomoć kako bi se izbeglo nezakonito regrutovanje i zlostavljanje.

Facebook je takođe prijavio stvaranje prečice za pružanje informacija i dodatnih resursa ljudima koji pretražuju termine koji se odnose na trgovinu ljudima u cilju seksualne eksploatacije. Takve termine su razvili interni i eksterni stručnjaci.

Da bi ublažio problem nedovoljnog prijavljivanja, Facebook je naveo da rade na „proaktivnom pronalaženju i preduzimanju mera u vezi sa sadržajima koji se odnose na trgovinu ljudima". Oni su prijavili „povećanje" njihove sposobnosti za „otkrivanje sadržaja koji krše pravila što predstavlja direktan rezultat velikih ulaganja naših tehničkih i operativnih timova".

IBM i Stop the Traffik, NVO sa sedištem u Ujedinjenom Kraljevstvu, udružili su se 2014. godine kako bi stvorili platformu Traffik Analysis Hub – novi subjekat koji vodi **zajedničku platformu za deljenje podataka** zasnovanu na bezbednom oblaku i analitici višejezičnog sadržaja zasnovanoj na veštačkoj inteligenciji i geoprostornoj analitici. Platforma okuplja 95 organizacija iz celog sveta. Cilj platforme je da poremeti globalnu trgovinu ljudima time što okuplja NVO (npr. StopTheTraffik, LibertyShared, CrimeStoppers i Save The Children UK), agencije za sprovođenje zakona (npr. Evropol, Interpol i razne policijske organe SAD) i finansijske institucije (npr. Western Union, Barclays, Standard Chartered, Lloyds i Paypal). Kao što je primetio IBM, platforma Traffik Analysis Hub koristi prilagođene modele veštačke inteligencije specifične za domen za prikupljanje relevantnih podataka u velikom obimu i za klasifikaciju ovih podataka na osnovu klasifikacije koju je razvila stručna zajednica platforme. Podaci se zatim dele među organizacijama učesnicama. Jedan od ključnih rezultata je „Red-Flag Accelerator", biblioteka tipologija razvijena na osnovu transakcija koje su označene znakovima upozorenja primećenim na računima žrtava. Ovakvi indikatori znakova upozorenja treba da budu implementirani u sisteme praćenja finansijskih institucija koje učestvuju u projektu. Pored toga, platforma ima za cilj da razvije alat za predviđanje zasnovan na korelaciji koji pomaže da se identifikuju karakteristike zajednica u riziku koje mogu da postanu izvori trgovine ljudima.

IBM je takođe primetio nedavno pokrenutu, **besplatnu onlajn mapu puta za obuku** onih koji su zainteresovani da postanu analitičari podataka u domenu trgovine ljudima. Obuka obuhvata module o trgovini ljudima (uvod u trgovinu ljudima; kako uočiti znakove trgovine ljudima), kao i module o nauci o podacima i primeni tehnologija u svrhu analitike podataka.

IBM takođe sponzoriše onlajn DataJam takmičenja tokom kojih stručnjaci IBM-a rade sa timovima iz različitih sektora na osmišljavanju inovacija u primeni tehnologije za sprečavanje trgovine ljudima. Neki od primera uključuju sledeće:

- Alati za „struganje" stranica za oglašavanje za odrasle na internetu i primenu markera prinudnog učešća (npr. jezik treće strane, više oglasa koji koriste iste identifikatore za kontakt, oglasi koji se odnose na istorijski poznate nacionalnosti žrtava) i izvođenje geo-prostorne analize klastera na oglasima „od interesa".
- Alati za „struganje" poruka na tržištima i forumima u dubokoj/mračnoj mreži, primenjuju markere specifične za trgovinu ljudima putem veštačke inteligencije, identifikuju teme u trendu i oznake korisnika, kreiraju mrežne modela tema za dalju analizu od strane agencija za sprovođenje zakona.
- Alati za validaciju oglasa za posao na internetu za pametne telefone, koji omogućavaju pojedincima da provere legitimnost oglasa za posao objavljenog na internetu pre uspostavljanja kontakta.

Kada je reč o **saradnji sa agencijama za sprovođenje zakona**, Facebook je naveo niz javno-privatnih partnerstava (JPP) u kojima učestvuje, kao što je Interpolova ekspertska grupa za trgovinu ljudima (HTEG) koja se bavi borbom protiv eksploatacije ljudi. Kao dodatni primer, Facebook je izvestio o primeni sistema onlajn zahteva za organe za sprovođenje zakona („LEORS") kako bi se pojednostavili pravni zahtevi za podatke o Facebook nalozima (uključujući zahteve koji se odnose na trgovinu ljudima). Zahteve podnete preko sistema LEORS rešavaju timovi sa sedištem u Sjedinjenim Državama, Irskoj i Singapuru.

## 3.7. Dodatni dokazi prikupljeni na osnovu analize okruženja

Pored dokaza koje su pružile države ugovornice, NVO i tehnološke kompanije, studija je takođe uključivala kancelarijsko istraživanje trenutne baze dokaza o strategijama i alatima koji se koriste za borbu protiv trgovine ljudima posredstvom interneta i tehnologije.

Organizacije OEBS i Tech against Trafficking (2020) sprovele su istraživanje IKT alata i inicijativa razvijenih za borbu protiv trgovine ljudima. One su e305 alata/inicijativa koje su razvile kompanije iz privatnog sektora, humanitarne organizacije i vlade (ogromna većina na engleskom jeziku). Među ovim alatima: 26% je dizajnirano za identifikaciju žrtava i trgovaca ljudima; 16% za podizanje svesti; 14% za upravljanje lancem snabdevanja; 13% za praćenje trendova i mapiranje podataka; 10% za identifikaciju korporativnog rizika; 9% za angažovanje i osnaživanje radnika i 12% za druge svrhe. Alati i inicijative koje su ispitali OEBS i Tech against Trafficking nastoje da postignu sledeći skup ciljeva: (a) širenje informacija u ugroženim zajednicama, uključujući migrante; (b) edukacija o rizicima trgovine ljudima, traženju pomoći i prijavljivanju potencijalnih slučajeva; (c) uklanjanje mogućnosti za eksploataciju; (d) identifikacija žrtava; (e) prikupljanje javno dostupnih informacija za borbu protiv trgovine ljudima; (f) procenu rizika od trgovine ljudima; (g) praćenje i usklađenost; (h) identifikovanje tipologija i postupanje na osnovu njih. Slično tome, Raets i Janssens (2018) su identifikovali sledeće (široke) načine na koje se alati zasnovani na tehnologiji mogu koristiti u borbi protiv trgovine ljudima: (a) agregacija i analiza podataka; (b) lanac blokova za sledljivost i poreklo (praćenje lanaca snabdevanja); (c) veštačka inteligencija (AI) i mašinsko učenje za postizanje velike računarske snage; (d) prepoznavanje lica (skeniranje mreže radi prikupljanja podataka); (e) tehnologija za žrtve i preživele: identifikovanje i pružanje podrške žrtvama, pristup na različitim jezicima. Muraszkiewicz (2018) je identifikovao skeniranje mreže radi prikupljanja podataka; analitiku podataka; prediktivno nadziranje; korišćenje lanca blokova; geografske informacione sisteme (GIS); onlajn baze podataka; i inicijative za grupno delovanje kao dodatne načine na koje se alati zasnovani na tehnologiji mogu koristiti u borbi protiv trgovine ljudima. Često je nejasno koji od ovih alata zaista funkcionišu, koji se mogu korisno proširiti i koji zaista donose koristi žrtvama trgovine ljudima (čini se da su neki od ispitanih alata dizajnirani da prikupljaju informacije koje je potom teško koristiti u praksi). Na osnovu informacija koje se koriste kroz tehnologiju treba delovati. U slučaju o kome su raspravljali Rende Taylor i Shih (2019), pokazalo se da se retko reaguje na izveštaje radnika podnete putem elektronske aplikacije za prijavu povratnih informacija o eksploataciji u lancima snabdevanja.

U literaturi se navodi da se tehnologija teško može koristiti kao zamena za praktično znanje na terenu. Štaviše, prema agencijama za sprovođenje zakona koje su intervjuisali Elliott i McCartan (2013), tehnologije mobilnih telefona, uključujući aplikacije, mogu biti deo alata za borbu protiv trgovine ljudima, ali nisu sveobuhvatno rešenje. Operativno posmatrano, pružaoci internet usluga se vide kao subjekti koji drže značajan deo elektronskih dokaza, pa je nekoliko izvora ukazalo na značaj bliske saradnje sa privatnim sektorom. Takva saradnja treba da obuhvati mehanizme koji olakšavaju pribavljanje dokaza, uklanjanje takvih dokaza kad god je to prikladno i brzo prijavljivanje organima za sprovođenje zakona u određenim slučajevima. Istovremeno, identifikovane su brojne prepreke za razmenu informacija između različitih aktera. To uključuje pitanja privatnosti i bezbednosti podataka. Takođe su upućeni pozivi za uvođenje zajedničkih međunarodnih (multilateralnih) standarda koji podržavaju saradnju između agencija za sprovođenje zakona, NVO i privatnog sektora.

Tek veoma mali skup specifičnih alata je više puta spomenut u nekoliko izvora. Ovi alati uključuju: (a) projekat Artemis kompanije Microsoft, koji je razvio alat za otkrivanje tehnika

vrbovanja tako što je kreirao ocenu rizika za razgovore zasnovanu na prošlim slučajevima, a zatim označio one najsumnjivije kako bi ih ljudski moderatori pažljivo ispitali; (b) PhotoDNK kompanije Microsoft, koji stvara jedinstveni digitalni potpis (heš) slike, koji se zatim koristi za otkrivanje seksualne eksploatacije dece.

Međunarodna konfederacija sindikata izveštava o kampanji za podizanje svesti koju vodi AidRom za pružanje informacija ljudima koji na internetu traže posao u inostranstvu. Ova kampanja je uključivala savete o tome kako primetiti sumnjive oglase i razvila je sledeće smernice: „1. Obratite pažnju na izvor objave. Većina specijalizovanih stranica za traženje posla ne proverava objave agencija za zapošljavanje. 2. Nikada ne prihvatajte ponudu koja je stigla od pojedinaca. 3. Pažljivo pročitajte ugovor o posredovanju. Ako plaćate naknadu, uverite se da znate za šta plaćate i šta prihvatate kao uslove. Kada se jednom potpiše, teško je — ili čak nemoguće — poništiti dogovor. 4. Zatražite što je više moguće detalja o poslu za koji se prijavljujete. 5. Ako posao deluje previše dobro da bi bio istinit... verovatno nije istinit!" Internet se koristi kao sredstvo za zaštitu od regrutovanja u svrhu zloupotrebe. Nije jasno koliko je ova kampanja trajala i da li je podignuta na viši nivo ili usvojena u drugim državama.

Dva projekta se takođe često navode kao primer dobre prakse: Spotlight organizacije Thorn i projekat Polaris, oba sa sedištem u SAD. Spotlight je alat zasnovan na internetu koji je razvijen da pomogne istražiteljima da identifikuju decu žrtve trgovine ljudima korišćenjem onlajn dokaza. Međutim, u javnom domenu ima veoma malo informacija o softveru. Projekat Polaris analizira podatke uglavnom prikupljene preko Nacionalne telefonske linije za borbu protiv trgovine ljudima, dopunjene drugim (neodređenim) izvorima informacija.

Grupno delovanje u svrhu otkrivanja žrtava navodi se kao građanska inicijativa omogućena tehnologijom, za koju se TraffickCam često smatra najboljim primerom. Od ljudi se traži da slikaju hotelske sobe kako bi se takve slike mogle koristiti za identifikaciju lokacija žrtava. Međutim, nije jasno da li su takve inicijative efikasne. Štaviše, mogu otvoriti pitanja privatnosti, kao i povećati potencijalni rizik od osvete. Dok se saveti korisnika smatraju veoma dragocenim, inicijative za grupno delovanje moraju biti pažljivo ispitane i uravnotežene u odnosu na rizik stvaranja virtuelnih (i nevirtuelnih) grupa osvetnika.

Uopšteno govoreći, organizacija ICAT (2019) je identifikovala brojne načine kako tehnologija može da igra pozitivnu ulogu u borbi protiv trgovine ljudima. Oni uključuju: (a) pomaganje tokom istraga; (b) unapređenje krivičnog gonjenja; (c) podizanje svesti; (d) pružanje usluga žrtvama; i (e) bacanje novog svetla na strukturu i funkcionisanje mreža za trgovinu ljudima. Različiti izvori su ukazivali na značaj „**digitalnih otisaka**", što znači da onlajn sadržaji i povezani uređaji predstavljaju izuzetno bogat izvor informacija (Myria 2017; Mitchell i Boyd 2014). Ono što je najvažnije, moguće je mapirati **kriminalne mreže** na osnovu stranica društvenih mreža (Myria 2017; takođe ICAT 2019 i TRACE 2015). Prikupljanje i analiza digitalnih dokaza mogu da **smanje teret za žrtve** prilikom pružanja dokaza protiv trgovaca ljudima (kao i dokaza u njihovoj odbrani).

# 4. Obuka: šta je obezbeđeno, šta je potrebno

## 4.1. Obuka za organe za sprovođenje zakona: šta je obezbeđeno i šta je potrebno

Studija je prvo istražila obuke koje se trenutno pružaju organima za sprovođenje zakona u pogledu otkrivanja i istraživanja slučajeva trgovine ljudima posredstvom interneta i tehnologije. Zatim je izvršena „analiza potreba" kako bi se identifikovale dodatne potrebe za obukama koje bi se mogle ponuditi kako bi se povećala efikasnost otkrivanja, vođenja istraga i identifikacije žrtava.

Uopšteno govoreći, različite države pružaju različite nivoe obuka za organe za sprovođenje zakona, u različitim formatima. Sve u svemu, velika većina država je prijavila da organizuje obuke o trgovini ljudima. Međutim, publike za koje su takve obuke namenjene variraju od države do države, pri čemu neke zahtevaju da svi policijski službenici koji bi mogli doći u kontakt sa potencijalnom žrtvom prođu takvu obuku, dok drugi ograničavaju obuku na specijalizovane jedinice.

Koji su elementi obuka koje države smatraju ključnim u smislu trgovine ljudima posredstvom interneta i IKT? Postoji opšta saglasnost o činjenici da službenici treba da prođu obuku o (a) načinu otkrivanja slučajeva trgovine ljudima i žrtava; (b) načinu prikupljanja, čuvanja i obrade **elektronskih dokaza**, uključujući metode izdvajanja informacija iz računara i drugih digitalnih medija; i (c) načinu korišćenja relevantnih delova softvera, uključujući **analizu velikih količina podataka** i sistema za skeniranje mreže radi prikupljanja podataka (gde to dozvoljava nacionalno zakonodavstvo). Nekoliko država smatra da je neophodna **obuka o OSINT-u**. Istražne tehnike koje uključuju **tajne istrage na internetu** takođe se smatraju ključnim.

Iako je većina država prijavila obezbeđivanje elemenata ovih obuka, one su takođe naglasile probleme, uključujući (a) potrebu da se obuka održi aktuelnom i, u nekim slučajevima, da se značajno unaprede postojeći elementi; i (b) potrebu da se poveća udeo osoblja koje prolazi obuku. Neke države su izrazile zabrinutost zbog ograničenih obuka koje se često pružaju kada je reč o pitanjima povezanim sa IKT i, još više, trgovinom ljudima posredstvom IKT. Predloženo je da se **osmisle i obezbede intenzivni kursevi obuke o trgovini ljudima posredstvom IKT,** koji bi takođe obuhvatali i tehnička pitanja. Opet, različite države bi se našle u različitom položaju u odnosu na digitalne kompetencije svog osoblja za sprovođenje zakona, ali je jedan broj država ukazao na potrebu da ponude **dalju obuku o upotrebi IKT** kako bi se poboljšalo otkrivanje slučajeva trgovine ljudima.

Države su takođe istakle potrebu da se obezbedi i početna i kontinuirana obuka, uzimajući u obzir istražno okruženje koje se brzo menja. Ovo, sa druge strane, zahteva resurse za pripremu modula obuke (uključujući istraživanje o novim razvojima u kontekstu trgovine ljudima posredstvom IKT) i njihovu realizaciju.

Nije neuobičajeno da države ugovornice imaju službenike koji pohađaju module obuke koje organizuju međunarodne organizacije ili druge države. Razmena informacija i znanja na međunarodnom nivou je svakako dobra praksa. Pored toga, za države sa ograničenim budžetima i resursima, koristi mogu biti značajne. Međutim, pošto su neki elementi obuke i dalje u velikoj meri specifični za kontekst, postoji potreba da sve države budu u poziciji da interno razvijaju znanje i da organizuju obuke koje takođe uzimaju u obzir lokalne specifičnosti ove pojave

(ograničen broj država trenutno ne organizuje nikakve obuke o trgovini ljudima posredstvom IKT, uključujući o OSINT, već se oslanja samo na obuke koje pružaju spoljne organizacije).

Različite države imaju različite organizacione strukture, posebno kada se odlučuje o tome gde se nalazi znanje o IKT. Međutim, ključno je napomenuti značaj izbegavanja uskih grla u svakodnevnim operacijama zbog neoptimalne raspodele veština. Na primer, važno je da **znanje nije tako strukturisano da se ne razmenjuje**, jer to ometa efikasnost istraga. Predviđeno rešenje je razmišljanje o dvosmernom sistemu obuke između službenika specijalizovanih za borbu protiv trgovinu ljudima i službenika specijalizovanih za IKT. Druga strategija je širenje određenog stepena veština u oblasti IKT među različitim jedinicama, uključujući i jedinice za borbu protiv trgovine ljudima. Gledajući u budućnost, **rizik od uskih grla** je posebno akutan. S obzirom da će se zločini posredstvom IKT, uključujući trgovinu ljudima, verovatno povećavati, postoji potreba da se ne oslanjamo previše na centralizovane centre za borbu protiv visokotehnološkog (sajber) kriminala. U idealnom slučaju, takve centre bi trebalo pozivati samo u slučajevima koje karakteriše veoma visok nivo tehnološke sofisticiranosti – što ne izgleda kao tipičan slučaj trgovine ljudima posredstvom IKT. Kako bi se izbegla uska grla u sistemu, ključno je uključiti opšta/osnovna **znanja o visokotehnološkom kriminalu u rutinske obuke** koje se pružaju za istražitelje, a ne da se ovo posmatra kao skup „specijalizovanih" veština.

Na osnovu dokaza dobijenih od država ugovornica, možemo identifikovati šest širokih oblasti koje se smatraju kritičnim za razvoj kapaciteta. Oni uključuju:

- Prikupljanje i analizu informacija iz otvorenih izvora (OSINT).
- Prikupljanje podataka sa profila na društvenim mrežama i aplikacijama za komunikaciju, kao i sa mračne/TOR mreže.
- Ispitivanje informacija koje se nalaze na uređajima za komunikaciju i čuvanje informacija, uključujući informacije koje su korisnici izbrisali, kao i znanje o šifrovanju.
- Sposobnost potkrepljivanja podataka dobijenih iz IKT izvora dodatnim dokazima stečenim tokom krivične istrage.
- Identifikacija žrtava/potencijalnih žrtava u onlajn okruženju.
- Obuka o ekonomskom i finansijskom kriminalu sa elementom posvećenim onlajn transakcijama i potencijalno kriptovalutama.

### 4.1.1. Dizajniranje budućih obuka i dobrih praksi

Dokazi pribavljeni od država ugovornica ukazuju na niz konkretnih inicijativa koje bi se mogle usvojiti kako bi se ojačale odredbe o obukama u kontekstu trgovine ljudima posredstvom interneta i tehnologije. U nastavku su navedeni neki predlozi o dizajnu budućih modula obuke.

- Kreiranje studija slučaja i scenarija zasnovanih na trgovini ljudima koji će biti uključeni u **obuku o „digitalnoj istrazi".** Takva obuka se može podeliti na dva nivoa: Nivo 1 bi se mogao organizovati za sve službenike na prvoj liniji, dok bi nivo 2 mogao uključivati napredne obuke koje se organizuju za manji broj polaznika. Moguće je da bi barem deo ovih obuka bio organizovan u obliku učenja u manjim grupama kako bi se podstakla razmena ideja i diskusija o praksi.
- **Dodavanje elementa IKT u postojeće obuke o trgovini ljudima**. Iako je nekoliko država pomenulo organizovanje obuka o trgovini ljudima, samo nekolicina je izričito ukazala na uključivanje elemenata fokusiranih na IKT u ove obuke. Kako se sve više interakcija odvija na internetu, ključno je uključiti elemente IKT u „tradicionalne" obuke o trgovini

ljudima. Tehnička obuka može da uključuje elemente o najboljim praksama u istraživanju trgovine ljudima posredstvom IKT, kao i o nacionalnim i međunarodnim iskustvima.

- Organizovanje zajedničkih obuka koje uključuju više država i koje su osmišljene imajući u vidu aktuelne trendove. Na primer, ako postoje dokazi da se žrtve obično regrutuju u državi A, a zatim eksploatišu u državi B, moglo bi biti korisno organizovati zajedničku obuku koja uključuje službenike iz država A i B. Po ugledu na zajedničke istražne timove (ZIT), mogli bismo označiti takve aktivnosti kao **ZAO („Zajedničke aktivnosti obuke")**.
- Izbor službenika bez policijskih ovlašćenja koji poseduju tehničke veštine. Ti službenici mogu da integrišu specijalizovane jedinice (npr. jedinice za borbu protiv trgovine ljudima), da interno razvijaju znanja o tehničkim pitanjima IKT i da ih šire unutar jedinice/organizacije.
- Organizovanje zajedničkih obuka koje **okupljaju specijalizovane istražitelje i tužioce** kako bi se obe grupe aktera upoznale sa mogućnostima koje nude nove istražne metode, npr. korišćenje sajber infiltracije ili tajnih operacija na internetu, kao i prikupljanje elektronskih dokaza (uključujući zaplenu virtuelne imovine). Takva obuka može da obuhvati i tehničke i pravne aspekte u cilju poboljšanja upotrebe novih metoda orijentisanih na IKT među istražiteljima i tužiocima.
- **Razmena znanja na međunarodnom nivou**, npr. kroz učešće u međunarodnoj/regionalnoj obuci fokusiranoj na specifične aspekte istrage trgovine ljudima posredstvom IKT (primeri koje navode države ugovornice uključuju seminar „Međunarodna saradnja u oblasti visokotehnološkog kriminala i elektronskih dokaza" u organizaciji Saveta Evrope i Zajedničkog projekta EU Cyber@East, održan 7–9. decembra 2020).

Države su navele niz konkretnih inicijativa kao primere dobrih praksi:

- U Austriji, Zajednička operativna kancelarija za borbu protiv trgovine ljudima i krijumčarenja ljudi (sektor u okviru Kriminalističke obaveštajne službe) organizuje obuke i seminare o trgovini ljudima, prekograničnoj trgovini prostitucijom i identifikaciji žrtava. Posebna obuka je organizovana za Policiju Austrije, pravosudne organe, Saveznu kancelariju za imigraciju i azil (BFA), Savezni upravni sud (BVwG), nadležne organe u oblasti finansija, inspekcije rada i usluge pravnog savetovanja o otkrivanju slučajeva trgovine ljudima na internetu, uključujući na društvenim medijima. Ono što je najvažnije, takva obuka je premašila granice organa za sprovođenje zakona i uključivala je inspekciju rada, savetodavne službe i nadležne organe u oblasti finansija. Osim toga, policijski službenici specijalizovani za IKT prošli su posebnu obuku fokusiranu na trgovinu ljudima u svrhu seksualne eksploatacije. S druge strane, službenici specijalizovani za IKT su pružali obuku kolegama specijalizovanim za trgovinu ljudima/prekograničnu trgovinu prostitucijom u Kriminalističkoj obaveštajnoj službi/CID. Ovo je dobar primer dvosmerne obuke o kojoj je ranije bilo reči – i pruža obrazac koji bi se potencijalno mogao koristiti i na drugim mestima.
- U Bugarskoj je 2020. godine organizovan niz specijalizovanih radionica za policijske službenike, tužioce i sudije gde se diskutovalo o istraživanju i krivičnom gonjenju slučajeva trgovine ljudima pomoću podataka iz otvorenih izvora, uključujući onlajn podatke.
- U okviru partnerskih sporazuma sa Rumunijom i Bugarskom u oblasti trgovine ljudima, Norveška će organizovati dve zajedničke aktivnosti obuke na temu obaveštajnih podataka iz otvorenih izvora (OSINT) za učesnike iz Rumunije i Norveške. Cilj obuke je da se poboljša sposobnost istražitelja u Norveškoj, Bugarskoj i Rumuniji da identifikuju i istraže trgovinu ljudima posredstvom IKT.
- U Grčkoj, obuke i obrazovne inicijative o visokotehnološkom kriminalu imaju dvosmerni pristup: (a) skup univerzitetskih kurseva za poboljšanje razumevanja visokotehnološkog kriminala među budućim generacijama naučnika i studenata prava, i (b) skup kraćih kurseva obuke za službenike za sprovođenje zakona, pravosudne organe i zaposlene u privatnom sektoru kako bi se poboljšalo njihovo razumevanje visokotehnološkog kriminala i unapredili njihovi svakodnevni odgovori.

- U Britaniji, organi za sprovođenje zakona imaju formalne standardne operativne procedure (SOP) ili druge smernice za proaktivno praćenje, otkrivanje, istraživanje i ometanje trgovine ljudima posredstvom IKT. Ovo uključuje: mapiranje onlajn platformi na kojima je rizik od trgovine ljudima visok; vođenje tajnih operacija na internetu; korišćenje specifičnih indikatora potencijalne trgovine ljudima na onlajn platformama; analizu i upravljanje prijavama primljenim putem telefonskih linija za prijavu seksualnog zlostavljanja i eksploatacije dece na internetu; upotreba specifičnih tehnoloških alata za borbu protiv trgovine ljudima. Pored toga, istražitelji prolaze obuku o tome kako da efikasno spoje informacije iz otvorenih izvora sa različitim oblicima obaveštajnih podataka.
- U Francuskoj, obuka prvog nivoa za policijske službenike uključuje module o osnovama digitalne istrage; anonimnosti, mračnim mrežama i virtuelnim valutama; analizi okruženja za izvršenje krivičnih dela visokotehnološkog kriminala; istraživanju interneta i društvenih mreža (ovo obično prati specijalizacija na određenu temu, na primer, prevara ili seksualno zlostavljanje dece); prvim osobama koje reaguju na visokotehnološki kriminal (tj. očuvanju digitalnog mesta zločina). Dalje specijalizovane obuke uključuju module o: istraživanju visokotehnološkog kriminala (prikupljanje, obrada i analiza dokaza sa mobilnih telefona i računara; sudskim istražnim aktima u vezi sa digitalnim tehnologijama, uključujući pravna pitanja, međunarodnu saradnju i istražne strategije); obuci za analitičare digitalnih tragova; prikupljanju telefonskih podataka; istragama pod pseudonimima. Trenutno je u fazi izrade jednonedeljna obuka posvećena borbi protiv trgovini ljudima u svrhu radne eksploatacije (sa ciljem da se organizuje u prvoj polovini 2022. godine). Ova obuka će uključivati modul posvećen korišćenju tehnoloških alata.

## 4.2. Obuka tužilaca i sudija

Prema dostavljenim dokazima, organizovanje obuka za tužioce i sudije u vezi sa trgovinom ljudima posredstvom IKT prilično je neujednačeno u različitim državama ugovornicama. Nekoliko država je navelo da trenutno ne organizuje nikakve obuke za pravosuđe o ovoj pojavi. Druge države organizuju opšte obuke o trgovini ljudima bez elemenata posebno fokusiranih na pitanja vezana za IKT. Druga grupa država je navela da organizuje obuke o tome kako se koriste međunarodni pravni instrumenti u kontekstu visokotehnološkog kriminala, npr. Budimpeštanska konvencija i srodno nacionalno zakonodavstvo i/ili o tome kako se razvijaju predmeti visokotehnološkog kriminala. Na kraju, grupa država je u svoje obuke uključila elemente kriptovaluta i znanja o specifičnim tehnološkim alatima. U idealnom slučaju, sve države bi trebale da teže **integrisanju obuke o trgovini ljudima u vezi sa IKT, upotrebi međunarodnih pravnih instrumenata u kontekstu visokotehnološkog kriminala**, kao i implikacijama upotrebe specifičnih tehnoloških alata prilikom istraživanja slučajeva trgovine ljudima (npr. sistemi za skeniranje mreže ili softver za dešifrovanje informacija).

Čini se da je manji broj država integrisao studije slučaja u vezi sa trgovinom ljudima u svoje obuke o visokotehnološkom kriminalu. Slično tome, manji broj država je naveo da organizuju obuke koje uključuju elemente trgovine ljudima i IKT.

Države su u svojim odgovorima na upitnik navele niz konkretnih inicijativa kao primere dobrih praksi:

- U Republici Moldaviji, tokom prve polovine 2021. godine, Nacionalni institut za pravosuđe je organizovao obuku za 110 polaznika koja je pokrivala aspekte istraga trgovine ljudima posredstvom IKT. Obuka je uključivala sesije o (a) „karakteristikama istraga i suđenja za krivična dela u vezi sa trgovinom ljudima i telesnim elementima"; (b) „karakteristikama

istraga i procesuiranju krivičnih dela u oblasti borbe protiv trgovine ljudima; (c) „karakteristikama istraga i suđenja u predmetima koji se tiču prekograničnog, transnacionalnog i organizovanog kriminala".

- U Bugarskoj, Tužilaštvo Vrhovnog suda je održalo seminare za istražitelje i tužioce o trgovini ljudima i upotrebi IKT u trgovini ljudima. Tužilaštvo smatra da su „posebno efikasne radionice koje vode stručnjaci iz oblasti IKT, koje predstavljaju praktične primere korišćenja softverskih programa, kao i mogućnosti i operativne alate za korišćenje mobilnih aplikacija u svrhu otkrivanja teških krivičnih dela".
- U Švedskoj postoje tužioci specijalizovani za IKT, od kojih se neki bave predmetima trgovine ljudima. Tužilaštvo organizuje internu obuku o vođenju istraga o krivičnim delima u vezi sa IKT (uključujući upotrebu kriptovaluta u kriminalnim aktivnostima). Brojni tužioci koji se bave predmetima trgovine ljudima prisustvovali su ovim obukama. Osim toga, Akademija za pravosudnu obuku, koja je deo švedske Nacionalne sudske uprave i odgovorna je za pravosudnu obuku sudija i drugog pravnog osoblja, organizuje obuku o krivičnim delima posredstvom IKT na različitim nivoima.
- Letonski nadležni organi su uputili na međunarodnu obuku o trgovini ljudima i visokotehnološkom kriminalu koju je organizovalo poljsko Tužilaštvo za tužioce specijalizovane za organizovani kriminal (21–23. oktobra 2019. godine u Krakovu).

Na kraju, nekoliko država je istaklo značaj unapređenja obuka za sudije i tužioce u vezi sa elektronskim dokazima.

### POLJE | Obuke za NVO

NVO pružaju ključne obuke i stručnost na osnovu svog svakodnevnog iskustva u pomaganju i savetovanju žrtava – uključujući policiju i ugrožene zajednice i pojedince. Međutim, NVO su izrazile potrebu da im organi za sprovođenje zakona i međunarodne organizacije organizuju obuke o najnovijim dostignućima u tehnološkom okruženju i u oblasti trgovine ljudima, uključujući promene u strategijama regrutovanja.

Takođe su istakli potrebu za obukama o najboljim praksama i razmenom iskustava među državama. Ovo je naročito relevantno za dizajniranje i koordinaciju kampanja koje uključuju države porekla i države odredišta.

Iako neke NVO imaju stručnjake za pitanja bezbednosti na internetu, generalno i dalje postoji nedostatak obuke o tehnologiji, uključujući i obuke o upotrebi posebnih alata za identifikaciju i pomoć žrtvama. Kako je istakla organizacija La Strada International, to je „zbog nedostatka resursa i kapaciteta" jer je „već teško prikupiti dovoljno sredstava za osnovne programe podrške".

# 5. Pravni instrumenti

Ovo poglavlje istražuje međunarodne pravne instrumente od značaja za borbu protiv trgovine ljudima posredstvom interneta i IKT. Pregled pravnih okvira specifičnih za državu koji se odnose na identifikaciju i uklanjanje sadržaja u vezi sa trgovinom ljudima, kao i domaćih pravnih instrumenata koji su uopšteno relevantni za borbu protiv trgovine ljudima, dostupan je u Veb prilogu.

## 5.1. Međunarodni pravni instrumenti

Države ugovornice su identifikovale određeni broj pravnih instrumenata koji su značajni za borbu protiv trgovine ljudima posredstvom IKT. Većina instrumenata je opšteg karaktera i ima za cilj borbu protiv trgovine ljudima, bez obzira na *modus operandi* trgovaca ljudima. Najrelevantniji instrument usmeren ka kriminalu posredstvom IKT je Budimpeštanska konvencija Saveta Evrope (Konvencija o visokotehnološkom kriminalu), koju nekoliko država ugovornica navodi kao „važan" alat. S obzirom na njen značaj, primena Konvencije o visokotehnološkom kriminalu u kontekstu trgovine ljudima razmatra se u posebnom odeljku u nastavku. Dodatni instrumenti koje su identifikovale države ugovornice su sledeći:

- Konvencija UN protiv transnacionalnog organizovanog kriminala i njen Protokol za sprečavanje, suzbijanje i kažnjavanje trgovine ljudima, posebno trgovine ženama i decom (2000.)
- Evropska konvencija SE o ekstradiciji (ETS br. 024)
- Evropska konvencija SE o uzajamnom pružanju pomoći u krivičnim stvarima (ETS br. 030)
- Konvencija SE o borbi protiv trgovine ljudima (CETS br. 197)
- Direktiva 2011/36/EU Evropskog parlamenta i Saveta od 5. aprila 2011. godine o sprečavanju i borbi protiv trgovine ljudima i zaštiti žrtava
- Akt Saveta od 29. maja 2000. godine kojim se u skladu sa članom 34. Ugovora o Evropskoj uniji uspostavlja Konvencija o uzajamnom pružanju pomoći u krivičnim stvarima između država članica Evropske unije.

O povezanim pitanjima seksualnog zlostavljanja dece:

- Konvencija SE o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja (Lanzarot konvencija, CETS br. 201)
- Direktiva 2011/93/EU Evropskog parlamenta i Saveta od 13. decembra 2011. godine o borbi protiv seksualnog zlostavljanja i seksualne eksploatacije dece i dečije pornografije
- Odluka Saveta Evropske unije od 29. maja 2000. godine o borbi protiv dečije pornografije na internetu 2000/375/PUP.

O radnoj eksploataciji:

- Međunarodna organizacija rada, Konvencija br. 189 i Preporuka br. 201 o dostojanstvenom radu domaćih radnika, 2011.
- Međunarodna organizacija rada, Protokol iz 2014. uz Konvenciju o prinudnom radu, 1930.

Pored toga, države ugovornice su identifikovale niz međunarodnih agencija i programa koji su od ključnog značaja za unapređenje međunarodne pravne saradnje, takođe u kontekstu trgovine ljudima posredstvom IKT. Oni uključuju:

- Interpol
    - Projekat IWOL (blokiranje domena koji se odnose na seksualnu eksploataciju dece)
- Evropol
    - EMPACT (trgovina ljudima)
    - Dani zajedničkog delovanja
- Evrodžast
- Selec (Centar za sprovođenje zakona u Jugoistočnoj Evropi).

Na kraju, niz specifičnih operativnih instrumenata proizilazi iz dokaza koje su dostavile države ugovornice. Ovaj skup uključuje sledeće instrumente:

- Zahtevi za pravnu pomoć
- Evropski nalog za hapšenje
- Evropski nalog za istragu
- Zajednički istražni timovi
- Sistem EU Prüm (razmena nacionalnih podataka o DNK, otiscima prstiju i registracijama vozila)
- EU evidencija imena putnika (PNR)
- Evropol SIENA
- Službenici za vezu
- Interpolov sistem za obaveštenja.

### 5.1.1. Nedostaci postojećeg okvira

Uopšteno posmatrano, države ugovornice su izrazile pozitivan i podržavajući stav o dostupnim pravnim instrumentima koji omogućavaju saradnju među državama u borbi protiv trgovine ljudima. Konvencije SE o (a) uzajamnom pružanju pravne pomoći i (b) o visokotehnološkom kriminalu smatraju se „najčešće" korišćenim instrumentima i, generalno, ocenjene su kao „adekvatne". Ipak, države ugovornice su identifikovale neke potencijalne nedostatke i oblasti u kojima bi se postojeće zakonodavstvo moglo poboljšati. Imajte na umu da ove praznine odražavaju – i dopunjuju – izazove vezane za istragu i krivično gonjenje trgovine ljudima posredstvom IKT o kojima je već bilo reči u Poglavlju 1 – i treba ih čitati zajedno sa takvom analizom.

Glavni nedostaci koje su identifikovale države ugovornice odnose se na:

- Odsustvo zajednički dogovorenog (standardizovanog) pravnog okruženja koje podržava razmenu između pružalaca internet usluga i nadležnih organa kada se bave specifičnim istragama.
- Odredbe koje omogućavaju blagovremeni odgovor privatnih kompanija na zahteve za dostavljanje podataka kako bi se izbegla duga kašnjenja u dostavljanju takvih podataka. Međutim, takve odredbe treba da uzmu u obzir da bi veoma kratki rokovi mogli da kazne manje pružaoce usluga u korist velikih pružalaca usluga jer ovi drugi mogu lakše da priušte skupe automatizovane sisteme i/ili usluge na poziv (kao što su istakli švajcarski nadležni organi).
- Odredbe kojima se primoravaju privatne kompanije da otkriju informacije na direktan zahtev/nalog druge države.
- Odredbe kojima se sprovode zajednička pravila o čuvanju podataka.

- Odredbe za olakšavanje prikupljanja svedočenja žrtava i korišćenje svedočenja u drugoj državi. Ovo bi ublažilo poteškoće sa kojima se države suočavaju u ubeđivanju žrtava da svedoče na suđenjima zbog niza razloga, uključujući mobilnost žrtava, poteškoće u njihovom lociranju i stalnu ranjivost.
- Odredbe u vezi sa šifrovanjem (npr. pružaoci usluga nisu u obavezi da uklone šifrovanje kada predaju materijale nadležnim organima).
- Pitanja u vezi sa transnacionalnim merama protiv veb lokacija na kojima se nalaze materijali koji se mogu povezati sa olakšavanjem eksploatacije žrtava. Ovo je posebno složeno pitanje jer je usko isprepleteno sa razlikama među državama ugovornicama u njihovom pristupu aktivnostima prostitucije – i različitim režimima usvojenim u različitim državama.
- Odredbe koje uvode obavezu stalnog praćenja od strane kompanija u njihovom čitavom lancu snabdevanja, ciljajući na primer na korišćenje IKT u kontekstu zapošljavanja (na primer, francuski Zakon br. 399/2017 o obavezi stalnog praćenja i Zakon o modernom ropstvu Ujedinjenog Kraljevstva iz 2015. godine kojim se uvodi obaveza transparentnosti u lancima snabdevanja).
- Upotreba terminologije koja ne dozvoljava uvek da se zakonodavstvo razvija paralelno sa promenama u modus operandiju trgovaca ljudima.
- Razlike u prenošenju krivičnog dela trgovine ljudima (prema Protokolu UN iz Palerma) u nacionalno zakonodavstvo. Ove razlike mogu da predstavljaju izazove za međunarodnu saradnju, na primer oko pitanja koja se odnose na nedostatak pristanka i prinudu žrtve.
- Evropski nalog za hapšenje smatra se vrednim sredstvom; međutim, neke relevantne države porekla su često izvan pravosudnog okvira EU.
- Evropskim nalozima za istragu (EIO) može da nedostaje fleksibilnost, npr. može se javiti potreba za novim EIO ako istraga krene u novim pravcima, a oni mogu biti podložni dugim rokovima za odgovor.
- Zajednički istražni timovi (ZIT) smatraju se „efikasnim" sredstvom; međutim, oni mogu biti (a) složeni za sprovođenje; i (b) zahtevaju identičnu istragu u partnerskoj državi ili u više njih.

## 5.2. Budimpeštanska konvencija (o visokotehnološkom kriminalu) i borba protiv trgovine ljudima posredstvom IKT

Među državama ugovornicama postoji opšta saglasnost o značaju Konvencije o visokotehnološkom kriminalu – pri čemu je mnoge države navode kao „veoma značajan alat". Nekoliko država ugovornica smatra Konvenciju o visokotehnološkom kriminalu ključnim **alatom za podršku** u borbi protiv trgovine ljudima posredstvom IKT.

Prema dostavljenim dokazima, države ugovornice smatraju odredbe koje se odnose na **procesno pravo** najvrednijim u kontekstu trgovine ljudima posredstvom IKT (Poglavlje II, odeljak 2. Konvencije), a ne mere materijalnog krivičnog prava predviđene Poglavljem II, odeljak 1. Najvažnije je da oblast primene odredbi procesnog prava nije zavisan od izvršenja krivičnog dela navedenog u tački 1. poglavlja II. Predmeti trgovine ljudima posredstvom IKT verovatno će potpasti ili pod „krivična dela počinjena pomoću računarskog sistema" ili, u najmanju ruku, u dela koja zahtevaju „prikupljanje dokaza u elektronskom obliku" (član 14, stav 2). Slično tome, član 23. navodi da se principi koji podržavaju međunarodnu saradnju u kontekstu Konvencije primenjuju na „istrage ili postupke koji se tiču krivičnih dela u vezi sa računarskim sistemima i podacima, *ili* u svrhu prikupljanja dokaza o krivičnom delu u elektronskoj formi" (dodat kurziv). Države ugovornice su istakle **značaj da se procesne mere ne ograniče samo na krivična dela koja su izričito navedena** (npr. ona u Poglavlju II,

Odeljak 1). Međutim, izgleda da se ne slažu baš sve države oko ovog šireg tumačenja oblasti primene Konvencije.

Konvencija jasno ostvaruje svoj puni potencijal samo kada nije ograničena na krivična dela koja su izričito navedena u Poglavlju II, odeljak 1. Ovo je naročito tačno u kontekstu trgovine ljudima posredstvom IKT. Kao što su primetili nadležni organi Finske, između ostalog, „odredbe materijalnog krivičnog prava iz Budimpeštanske konvencije [koje] pokrivaju krivična dela u vezi sa računarom, kao što su nezakonit pristup, menjanje podataka, računarsko falsifikovanje i kršenje autorskih prava i druga slična krivična dela, retko su relevantne ili uopšte nisu relevantne u kontekstu trgovine ljudima". Naprotiv, nekoliko država ugovornica je navelo da su se oslanjale na odredbe Konvencije o čuvanju podataka u kontekstu istraga trgovine ljudima (posebno na članove 16–21).

Nekoliko država je ukazalo na korisnost odredbi navedenih u Poglavlju III Konvencije (o međunarodnoj saradnji) kao pravnom osnovu za prikupljanje i razmenu elektronskih dokaza među državama. Mehanizmi uzajamne pomoći predviđeni Poglavljem III Konvencija (članovi 29–34) smatraju se „korisnim". Nekoliko država je izričito naznačilo da su se ranije oslanjale na njih. Članovi 29. i 31. se najčešće pominju; član 30. nije izričito pomenut u prijavama; ipak, mogao bi da ponudi koristan alat u kontekstu trgovine ljudima posredstvom IKT.

Uspostavljanje **mreže kontaktnih tačaka** dostupnih 24/7 (član 35.) takođe se smatra važnom odredbom, posebno u kontekstu prikupljanja elektronskih dokaza. Ključno je, međutim, da kontaktne tačke budu lako dostupne iz svake države. Ovo govori o problemu **uskih grla unutar sistema**. Ključno je mesto gde se kontaktna tačka nalazi u sistemu krivičnog pravosuđa – i to može biti od velikog značaja. Primenjuju se različiti modeli. U Republici Moldaviji, na primer, takva kontaktna tačka se nalazi pri Upravi za istrage visokotehnološkog kriminala; na Malti pri Policijskoj jedinici za visokotehnološki kriminal i, u Poljskoj, pri Birou za borbu protiv visokotehnološkog kriminala Centralnog štaba nacionalne policije. U Francuskoj se nalazi pri Centralnoj kancelariji za borbu protiv kriminala u oblasti informacionih i komunikacionih tehnologija (OCLCTIC), dok se u Letoniji takva kontaktna tačka nalazi pri Odeljenju za međunarodnu saradnju državne policije. Nadležni organi u Bosni i Hercegovini su izričito naveli svoje „veoma pozitivno iskustvo" usled činjenice da se kontaktna tačka dostupna 24/7 „ne nalazi u jedinici koja se bavi visokotehnološkim kriminalom". Gledajući u budućnost, verovatno je da će, sa sve centralnijom ulogom koju igraju IKT i elektronski dokazi, takve kontaktne tačke biti pod sve većim pritiskom – i brzo preopterećene, ako ne budu imale adekvatno osoblje. Samostalne jedinice za podršku bi možda bile poželjnije od jedinica za visokotehnološki kriminal – idealno sa osobljem koje poseduje stručnost u različitim oblastima i vrstama kriminala, uključujući trgovinu ljudima posredstvom IKT. Međutim, bez obzira na izabrani model, država treba da vodi računa o pitanju uskih grla.

### 5.2.1. Pogled u budućnost: kako se Konvencija o visokotehnološkom kriminalu može dalje primenjivati u borbi protiv trgovine ljudima

Nekoliko država je istaklo značaj Drugog dodatnog protokola uz Konvenciju. U nekoliko prijava je navedeno da će Drugi dodatni protokol stvoriti vredne alate za organe za sprovođenje zakona – koji će se koristiti i u kontekstu trgovine ljudima posredstvom IKT – što će unaprediti prekogranične krivične istrage i dalje unaprediti saradnju u vezi sa obezbeđivanjem elektronskih dokaza. Članovi koji su istaknuti kao posebno relevantni uključuju odredbe koje se odnose na zajedničke istrage, uključujući zajedničke istražne timove; ubrzano otkrivanje sačuvanih računarskih podataka; hitna uzajamna pomoć i direktno otkrivanje informacija o pretplatnicima.

Osim toga, države ugovornice su predložile sledeće aktivnosti za poboljšanje borbe protiv trgovine ljudima posredstvom IKT kroz primenu konvencija o visokotehnološkom kriminalu:

- Potpuno usaglašavanje svih nacionalnih zakonodavstava sa Konvencijom o visokotehnološkom kriminalu kako bi se iskoristio puni potencijal koji ova konvencija nudi.
- Šira i poboljšana obuka o mogućnostima koje nudi Konvencija o visokotehnološkom kriminalu. Iz prijava proizilazi da trenutno ne koriste sve države ugovornice alate predviđene Konvencijom u njihovom punom potencijalu.
- Više jasnoće u vezi sa oblašću primene odredbi procesnog prava koje su već uključene u Konvenciju i njene Dodatne protokole jer se pojavio određeni stepen neslaganja među državama ugovornicama o tome u kojoj meri se postojeće odredbe mogu primeniti na slučajeve trgovine ljudima. Dok neke države ugovornice smatraju da, sve dok pokriva elektronske dokaze, Konvencija o visokotehnološkom kriminalu može biti u potpunosti primenjena, druge države su upozorile da primena Konvencije i Protokola, uključujući Drugi dodatni protokol, zahteva „prikladne predmete" (u prijavama nije navedeno šta čini predmet „prikladnim").
- Neke države ugovornice su izrazile stav da Drugi dodatni protokol treba da uključi odredbe koje jačaju razmenu elektronskih dokaza, poboljšavaju modalitete uzajamne pravne pomoći, podstiču saradnju sa pružaocima internet usluga i poboljšavaju prekogranični pristup podacima.
- Manji broj država ugovornica smatra da Konvenciju o visokotehnološkom kriminalu treba dopuniti ili izmeniti kako bi izričito predviđala trgovinu ljudima u svojoj oblasti primene. Bugarski nadležni organi su izrazili potrebu za izradom „kataloga krivičnih dela" na koja se mogu primeniti alati sadržani u Konvenciji o visokotehnološkom kriminalu i Dodatnim protokolima. Međutim, čini se da ovo gledište nije opšte prihvaćeno među državama ugovornicama jer se čini da postoji opšta preferencija za šire tumačenje oblasti primene Konvencije zasnovano na (širokom) zahtevu „prikupljanja dokaza u elektronskom obliku" (videti takođe iznad).
- Slovački nadležni organi su predložili sprovođenje procedure za ubrzanje pružanja UPP pružanjem mogućnosti da se zahtev pošalje direktno subjektu koji se nalazi u stranoj državi pod uslovom da se o tome obavesti pravosudni organ te države.

## POLJE | Izazovi koje su identifikovale NVO

Uopšteno govoreći, NVO smatraju da su izazovi uglavnom posledica sprovođenja postojećih odredbi, uključujući i nedostatak resursa koji su na raspolaganju organima za sprovođenje zakona i organizacijama za podršku, a ne po slovu važećih zakonskih odredbi.

Organizacija La Strada International je primetila „**jasna ograničenja" koja su uvedena zakonodavstvom o zaštiti podataka (GDPR) i pravilima privatnosti**. Primer je „zakon o e-privatnosti koji je predložila EU a koji je sprečio tehnološke kompanije da skeniraju internet u potrazi za slučajevima seksualne eksploatacije dece na internetu" (sada privremeno suspendovan nakon protivljenja mnogih OCD). Organizacija Sustainable Rescue Foundation je ukazala na „jasan prelaz sa fizičkih dokaza na digitalne podatke" koji stvara potrebu za „digitalnom forenzikom kao prihvatljivim dokazom za policiju i tužioce" u svim državama. Ostali izazovi koje su prepoznali odnose se na GDPR u EU; ažuriranje propisa i sudske prakse tako da uzimaju u obzir visokotehnološki kriminal i internet; osmišljavanje zakonodavstva i operativnih pravila prilagođenih digitalnim istragama.

Fondacija Sustainable Rescue Foundation je takođe predložila da se zakonodavstvo protiv finansijskog kriminala razmotri kao rešenje za problem pretvaranja informacija u prihvatljive dokaze. Na primer, Južnoafrička integrisana radna grupa za borbu protiv pranja novca, koja predstavlja partnerstvo između javnih subjekata i finansijskog sektora, može da podnese zahtev za izdavanje sudskog naloga kojim bi se odobrio pristup relevantnim informacijama koje se nalaze u posedu finansijskih i drugih institucija. Putem izjave pod zakletvom, ove informacije (tj. finansijske analize finansijskih podataka dobijenih posredstvom suda) mogu zatim da koriste agencije za sprovođenje zakona.

# 6. Ljudska prava, etika i zaštita podataka

## 6.1. Dokazi prikupljeni od država ugovornica

Što se tiče **obrade i zaštite podataka**, sve države ugovornice su ukazale na usvajanje zakona o zaštiti podataka – koji su često usklađeni sa Uredbom EU 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. godine (koja se takođe naziva Opštom uredbom EU o zaštiti podataka o ličnosti: GDPR) i/ili Konvencijom SE o zaštiti lica u odnosu na obradu podataka o ličnosti (ETS br. 108, revidirano 2018. godine kao verzija 108+). Principi zaštite podataka slični su u svim državama ugovornicama. To uključuje zakonitost, ograničenje svrhe, minimiziranje i srazmernost podataka, tačnost, ograničenje čuvanja, integritet i poverljivost. Nije moguće izvršiti evaluaciju sprovođenja takvih principa na osnovu dokaza pruženih u odgovorima na upitnik.

Što se tiče **ljudskih prava** i **lične zaštite žrtava**, jedan broj država je ukazao na uvođenje mera za sprečavanje počinilaca da stupe u kontakt sa žrtvama; ispitivanje svedoka putem video-konferencije kako bi se sprečio kontakt sa optuženima; a u nekim slučajevima i mogućnost da žrtve anonimno pruže dokaze na sudu kako bi se zaštitila njihova anonimnost. Žrtve se mogu smestiti u **skloništa** i može im se pružiti pomoć.

U Francuskoj, korisnici platforme za prijavljivanje seksualnog i rodno zasnovanog nasilja moraju da **daju saglasnost za prikupljanje podataka o ličnosti** kada se prvi put povežu sa platformom. Ova saglasnost se obnavlja tokom razgovora. Međutim, nije obavezno da se navede identitet pojedinca da bi se pristupilo sobi za ćaskanje – na taj način se omogućavaju anonimni kontakti.

Što se tiče **podataka prikupljenih tokom policijskog rada**, uključujući istrage, države ugovornice su istakle da zakoni i propisi obično propisuju da su takve informacije podložne poverljivosti i da se mogu deliti samo u veoma ograničenim okolnostima uz stroge procedure i ovlašćenja. Države ugovornice su navele da su pravila prema kojima policijske snage mogu da registruju podatke u određenim bazama podataka obično usklađena sa Direktivom o policiji EU. Pojedinačne države mogu imati strože nacionalne zahteve. Kako su istakli norveški nadležni organi, posebne kategorije podataka o ličnosti, na primer, o seksualnoj orijentaciji, veroispovesti i političkim stavovima, mogu biti predmet dodatnih zahteva i „mogu se obrađivati samo kada je „strogo neophodno" u prethodno utvrđene svrhe". Isti skup pravila i zaštitnih mera najčešće pokriva sve istrage i obaveštajni rad, uključujući one koji uključuju trgovinu ljudima posredstvom IKT. Od ključnog je značaja da osoblje za sprovođenje zakona bude adekvatno obučeno o regulatornim i etičkim odredbama koje uređuju obradu podataka o ličnosti.

Rad policije takođe treba da **postigne ravnotežu između različitih potreba i prava**. Na primer, kako su primetili finski nadležni organi, nalog kojim se ograničava pristup elektronskoj komunikaciji „može se izdati samo ako se koristi od zabrane pristupa informacijama mogu smatrati znatno većim od ograničenja slobode izražavanja i drugih osnovnih prava korisnika mreže" (član 185. Zakona o elektronskim komunikacionim uslugama 917/2014). Pored toga, mora biti „tehnički sproveden na takav način da zaštita poverljivosti komunikacije ne bude ugrožena". Uopšteno govoreći, član 226c istog zakona propisuje da „mere koje se odnose na uslove korišćenja platformi za deljenje video-zapisa moraju biti srazmerne prirodi predmetnog sadržaja i moraju uzeti u obzir, na primer, potencijalnu štetu i prava pružalaca usluga i

korisnika". Finski nacionalni istražni biro je sam identifikovao probleme privatnosti u vezi sa korišćenjem eksternih tehničkih alata i prijavio ih je Odboru nacionalne policije.

Države ugovornice su navele da imaju uspostavljene **starosno osetljive protokole** koji se odnose na različite skupove procedura i zaštitnih mera koje se primenjuju u zavisnosti od toga da li je žrtva dete. Na primer, deca su obično smeštena u zasebnim centrima za podršku; koriste se različite tehnike i sobe za ispitivanje, često uz prisustvo psihologa. U nekim državama, krivične postupke protiv dece vode isključivo policijski službenici posebno obučeni za rad sa decom i maloletnicima.

## 6.2. Dokazi prikupljeni od NVO

NVO su naglasile značaj pravila – i svest o pravilima – za zaštitu podataka, poverljivosti, bezbednog čuvanja, kao i procedura oko pristanka.

Dokazi nekoliko NVO pokazuju da, u okviru standardne procedure, organizacije traže pristanak žrtve pre nego što podele informacije sa organima za sprovođenje zakona. Kao što je istakao FIZ (Švajcarska), ova saglasnost se takođe odnosi na deljenje podataka o SIM kartici i akreditiva za društvene mreže. Organizacija La Strada International je navela da njeni članovi „ne prosleđuju nikakve informacije policiji bez pristanka žrtve, osim u slučaju postojanja opasne situacije u kojoj je potrebna hitna reakcija". Problem nastaje kada žrtve oklevaju da podnesu pritužbu policiji „zbog rizika koje to nosi, uključujući rizike da njihova situacija postane poznata drugima, pored rizika od odmazde". Organizacija La Strada International ocenjuje da je to slučaj sa „mnogim žrtvama trgovine ljudima".

Organizacija Different and Equal (Albanija) je pomenula upotrebu sigurnosnih protokola u svakoj komunikaciji sa agencijama za sprovođenje zakona, uključujući šifrovanje. Interni protokoli su uvedeni uzimajući u obzir potrebu da se sačuva poverljivost žrtava i zaštite njihovi podaci. Slično tome, organizacija FIZ (Švajcarska) je naglasila potrebu za zaštitom poverljivosti podataka kao uslova za dobru saradnju sa organima za sprovođenje zakona. Astra (Srbija) je istakla da je **poverljivost žrtava** „ključan deo našeg rada" i da odricanje od poverljivosti „nije i ne sme biti uslov za dobijanje podrške i pomoći". Organizacija KOK (Nemačka) je istakla da je „zaštita pojedinca jača od potrebe za prikupljanjem dokaza". Praksis (Grčka) tvrdi da, kada dele informacije sa organima za sprovođenje zakona u skladu sa pravilima o zaštiti podataka (deljenje zasnovano na pristanku), njihova „primarna briga je uvek neposredna i efikasna zaštita potencijalne žrtve".

Pitanja zaštite podataka i razmene podataka mogu da stvore **moralne dileme**. Kako je istakla organizacija La Strada International, deljenje podataka sa organima za sprovođenje zakona i podnošenje pritužbi podržavaju istrage, koje zauzvrat kasnije potencijalno mogu spasiti i zaštititi više žrtava. Međutim, to može da ima svoju cenu za pojedinačnu žrtvu, koja bi mogla biti izložena rizicima i pretnjama, uključujući socijalnu isključenost. Osim toga, mogu postojati problemi vezani za dugoročne efekte registracije žrtve i deljenja podataka o ličnosti, uključujući potencijalno krivično gonjenje i kažnjavanje od strane nadležnih organa (ovo se može pogoršati kada se žrtva nezakonito nalazi u državi u vreme registracije). I La Strada International i La Strada Moldova smatraju da pronalaženje prave ravnoteže između potrebe žrtava za poverljivošću u pristupu uslugama i potrebe za prikupljanjem dokaza za pomoć u borbi protiv trgovine ljudima u širem smislu može biti „veoma izazovno". Ovo je još akutnije kada je žrtva dete: kako je primetila La Strada Moldova, deca se često plaše da daju saglasnosti i podnesu zvaničnu pritužbu policiji, uključujući i zbog straha od reakcije svojih roditelja.

Prema navodima La Strada International, pravila o zaštiti podataka „otežala su razmenu podataka među NVO i drugih relevantnih aktera". Istovremeno, NVO su svesne da bi „žrtvama trgovine ljudima ili rizičnim grupama moglo biti teško da znaju koji se podaci čuvaju i/ili da obezbede da se podaci ispravljaju, blokiraju ili brišu i da koriste ovo pravo", uprkos postojanju protokola o zaštiti podataka.

Dalja pitanja proizilaze iz prikupljanja podataka o ličnosti na osnovu kojih se može izvršiti identifikacija putem **tehnika ekstrakcije podataka**. Sustainable Rescue Foundation (SRF) se osvrnula na dva zasebna projekta koji se trenutno sprovode u Holandiji: RIVET (SRF) i Lovitura 10 Elenas (laboratorija Policije Holandije). Oba projekta se fokusiraju na trgovinu Rumunkama u Holandiji radi seksualne eksploatacije. SRF RIVET koristi ekstrakciju podataka usmerenu na žrtvu na osnovu intervjua sa 10 rumunskih seksualnih radnica i istražuje upotrebu tehnologije za otkrivanje, prikupljanje, čišćenje i analizu podataka radi izgradnje taksonomija modus operandija. Lovitura 10 Elenas digitalno prati deset rumunskih seksualnih radnica kako bi se stekao uvid u način funkcionisanja kriminalnih mreža. Kako je istakao RSF, izazov je „osigurati [da] sve rumunske seksualne radnice koje učestvuju u oba projekta ostanu anonimne". Skloništa žele da zaštite anonimnost seksualnih radnika, a policija ne može da deli svoju operativnu bazu podataka. SFR je predložio korišćenje protokola za poređenje podataka za multilateralno računanje (MPC) kao moguće rešenje. Ovaj pristup se sastoji u anonimizovanju podataka koji potiču iz različitih skupova podataka (npr. NVO i policije) na takav način da ih onda mogu deliti i čitati različiti sistemi kako bi proverili, na primer, da li ima dupliranih imena.

La Strada International je pozvala da se posveti više pažnje potencijalnim rizicima i šteti koju stvaraju prikupljanja podataka (u velikim razmerama) i tehnološki alati, upozoravajući da je u ovom trenutku fokus samo „na pozitivnim aspektima i mogućnostima" takvih alata. Ista organizacija je takođe tvrdila da je „potrebna veća kontrola upotrebe podataka i njihovog bezbednog čuvanja, kao i da se obezbedi da se sva pravila zaštite podataka delotvorno primenjuju". Žrtve, rizične grupe i NVO treba da imaju „više mogućnosti [...] da odbiju zahteve za pružanje podataka i da maksimalno smanje prikupljanje podataka".

NVO imaju tendenciju da imaju različite protokole na osnovu toga da li je žrtva dete ili odrasla osoba (**starosno osetljivi protokoli**).

## 6.3. Dodatni dokazi prikupljeni na osnovu analize okruženja

IKT mogu da imaju značajan uticaj na **ljudska prava** pojedinaca, uključujući pravo na privatnost, slobodu izražavanja i zaštitu od diskriminacije. U literaturi su otvorena različita pitanja.

Na osnovu OEBS (2020), možemo navesti niz **etičkih pitanja** koja treba uzeti u obzir prilikom razvoja tehnologije za borbu protiv trgovine ljudima. To uključuje: (a) zaštitu privatnosti podataka; (b) protokole o saglasnosti koje potpisuju žrtve; (c) obuke za osobe koji rukuju osetljivim podacima, posebno podacima o žrtvama; (d) bezbedno čuvanje podataka; (e) sprečavanje upotrebe tehnologije za dobijanje osetljivih podataka o ranjivim ljudima (opšte prikupljanje podataka o ranjivim ili marginalizovanim populacijama, čime se stvara rizik od diskriminatornih praksi); i (f) korišćenje tehnologije na način koji ne krši ljudska prava žrtava, kao ni ljudska prava šireg stanovništva. ICAT (2019) takođe naglašava pitanja vezana za **privatnost podataka, etiku, transparentnost, odgovornost i informisani pristanak**. On naglašava potrebu da se osigura da se podaci bezbedno čuvaju; da postoje protokoli o saglasnosti; i da su podaci rodno i uzrasno osetljivi. Osim toga, informacije koje

objavljuju organi za sprovođenje zakona treba da se procene tako da žrtve i njihove porodice ne budu izložene riziku.

ICAT (2019) i drugi izvori su ukazali na osetljivost u vezi sa **deljenjem podataka**. Kada se podaci dele između država i/ili relevantnih agencija, to treba da se uradi u skladu sa načelima privatnosti i poverljivosti. Primećuje se da bi potencijalni sukob mogao nastati između potrebe za poverljivošću kada žrtve pristupaju uslugama i dobijaju podršku s jedne strane, i potrebe za informacijama/dokazima za izgradnju jake istrage, s druge strane. Gerry i drugi (2016) naglasili su značaj ključnih pravnih principa – principa poštenog informisanja – u vezi sa obradom podataka o ličnosti (ovo uključuje princip ograničenja svrhe). Predlaže se da takvi principi ostaju važni i u slučaju trgovine ljudima, a posebno u odnosu na žrtve.

Gerry i drugi (2016) su takođe upozorili na rizik koji donose široko rasprostranjeni **alati za praćenje** u borbi protiv trgovine ljudima. Iako takva tehnologija može da ponudi nove mogućnosti za intervenciju u situacijama trgovine ljudima, ona se takođe sastoji od **oblika nadzora koji potencijalno veoma zadire** u privatnost pojedinca. Kako navode, ova tehnologija „može da otkrije mnoštvo informacija u vezi sa njihovim privatnim životom, uključujući njihovu pripadnost određenoj veroispovesti, razvoj ličnih odnosa i druženja sa drugim pojedincima, kao i njihove svakodnevne navike", stavljajući tako ugrožene grupe u opasnost od diskriminacije i profilisanja. Opšte praćenje čitavih rizičnih populacija, npr. grupe migranata, može da ima ozbiljne posledice po privatnost pojedinaca. Gerry i drugi (2016) naglašavaju potrebu da se razviju **mehanizmi za utvrđivanje da li se tehnologija praćenja koristi preterano ili zloupotrebljava**. Oni predlažu izbegavanje sistema koji uključuju centralizovano čuvanje podataka o ličnosti žrtava ili potencijalnih žrtava. Uopšteno, alate za borbu protiv trgovine ljudima zasnovane na tehnologiji treba **razvijati i koristiti odgovorno i etički**. Takve zahteve treba uzeti u obzir u svim fazama, od razvoja do konačne upotrebe. Rešenja zasnovana na tehnologiji takođe treba proceniti na osnovu njihovog nivoa zadiranja u privatnosti ljudi. Neki naučnici, uključujući Milivojevića i druge (2020), upozorili su na potencijalne negativne posledice široke upotrebe tehnika prepoznavanja lica za marginalizovanu populaciju, i uopštenije za ono što definišu kao „moralni imperativ zaštite i spasavanja". Iako priznaju potencijal tehnologije kao pomoćnog sredstva u borbi protiv trgovine ljudima, oni takođe naglašavaju značaj stavljanja **najboljih interesa žrtava** u centar svake akcije.

Nekoliko izvora, uključujući Milivojević i drugi (2020) i Gerry i drugi (2016), ističe značaj **da se žrtvama ne uskraćuje mogućnosti korišćenja tehnologije**, jer pristup tehnologiji može biti njihov jedini način da komuniciraju sa spoljnim svetom i može da posluži kao važan mehanizam suočavanja. Uklanjanje pristupa tehnologiji može da obespravi žrtve; promovisanje bezbednog pristupa tehnologiji treba umesto toga da ima prednost.

Na kraju, u literaturi se **retko uvažava rodno zasnovana osetljivost**. Priznaje se da je vrsta eksploatacije rodno osetljiva, pri čemu su žene češće eksploatisane za seksualne usluge, rad u kući i ličnu negu, a muškarci češće u poljoprivredi, građevinarstvu i drugim zanimanjima koja zahtevaju manuelni rad (npr. ulična prodaja, pranje automobila). Osim toga, čini se da je vrbovanje putem interneta više povezano sa ženskim žrtvama nego sa muškim žrtvama; međutim, dokazi takođe sugerišu da bi druge ranjivosti mogle biti u igri u slučaju vrbovanja putem interneta, na primer da je osoba u ustanovi za negu (preliminarni dokazi iz Rumunije navedeni su u Di Nicola i drugi 2017).


# Preporuke

## Aktivnosti za poboljšanje otkrivanja slučajeva trgovine ljudima posredstvom tehnologije

1. Organi za sprovođenje zakona treba da ulažu u razvoj kapaciteta u oblastima **nadgledanja interneta, sajber patrola, tajnih istraga na internetu (sajber infiltracija), upotrebe podataka iz otvorenih izvora (OSINT) od strane specijalizovanih službenika, analize društvenih mreža** i upotrebe **alata za automatsko pretraživanje** za analizu dokaza. Razvoj i upotreba takvih alata moraju biti u skladu sa načelima vladavine prava. Države treba da razmotre prilagođavanje postojećeg zakonodavstva kako bi omogućile sajber patroliranje i tajne istrage na internetu (sajber infiltraciju) – uz pažljivo razmatranje etičkih implikacija. Nadležni organi takođe treba da razmotre ulaganje u alate za pomoć istražiteljima u rukovanju i obradi podataka u velikim razmerama (mogućnost za obradu velikih količina podataka). Resursi bi se mogli udružiti na nadnacionalnom nivou za razvoj tehnoloških proizvoda, kao što su sistemi za skeniranje mreže, kao i za razmenu stručnosti o njihovoj upotrebi.
2. Organi za sprovođenje zakona i inspekcije rada bi trebalo da sprovode **strože propise i češće kontrole na stranicama sa oglasima za posao**. Ovo bi se moglo postići uz podršku tehnoloških alata razvijenih u saradnji sa privatnim kompanijama (npr. alati za validaciju oglasa za posao na internetu, alati za „struganje" stranica sa oglasima za posao i upotreba markera trgovine ljudima). Inspekcije rada bi trebalo da **razviju digitalnu ekspertizu i povećaju svoje prisustvo na internetu**.

3. Države/privatni pružaoci usluga/NVO moraju da unaprede **mehanizme za poverljivo prijavljivanje putem interneta** koji omogućavaju anonimno prijavljivanje slučajeva trgovine ljudima, kao i samoidentifikovanje žrtava. Ćaskanje, uključujući čet-botove, i funkcije za razmenu poruka mogu biti dragoceni alati na internetu. Države bi trebalo da sarađuju sa privatnim kompanijama koje nude onlajn usluge kako bi **eliminisale mogućnosti za trgovce ljudima**, razvile **analitike sadržaja** za otkrivanje slučajeva trgovine ljudima i utvrdile lako dostupne mehanizme za klijente da prijave sumnjive aktivnosti/oglase. Tamo gde je dozvoljeno nacionalnim zakonodavstvom, ovo bi trebalo da se proširi na kompanije koje nude usluge za odrasle na internetu. Kompanije treba bezbedno da čuvaju onlajn sadržaje i informacije (npr. IP adrese) povezane sa prijavljenim aktivnostima/oglasima.

## Aktivnosti za poboljšanje istraga o trgovini ljudima posredstvom tehnologije

4. Organi za sprovođenje zakona bi trebalo da razmotre organizovanje obuka za službenike specijalizovane za IKT i trgovinu ljudima. Države bi takođe trebale da razmotre stvaranje **grupa za tehničku podršku** u kojima bi radili policijski službenici sa policijskim ovlašćenjima ili ostali policijski službenici sa specijalizovanim sposobnostima u oblasti IKT, koje bi bile integrisane u jedinice za trgovinu ljudima. Osim toga, države treba da preispitaju strukturu interne **raspodele digitalnih istražnih sposobnosti** kako bi predvidele i izbegle potencijalna **uska grla u istragama**. Kako će se zločini posredstvom IKT, uključujući trgovinu ljudima, verovatno stalno povećavati, nedostatak specijalizovanih službenika na lokalnom nivou i preveliko oslanjanje na pomoć (preopterećenih) centralizovanih jedinica za visokotehnološki kriminal će verovatno stvoriti uska grla.

5. Organi za sprovođenje zakona treba da se pobrinu da **svi službenici** poseduju odgovarajući nivo stručnosti za prikupljanje i rukovanje **elektronskim dokazima**. Obuka o elektronskim dokazima treba da bude sastavni deo nastavnih planova i programa obuke i da se neprekidno ažurira zbog brzog menjanja tehnološkog okruženja i ponašanja. Pošto je očuvanje elektronskih dokaza ključno za razvoj jakih istraga, **savetnici i NVO na prvoj liniji odbrane** takođe treba da budu upoznati sa strategijama za očuvanje digitalnih dokaza (npr. čuvanjem istorije ćaskanja).

6. Države/međunarodne organizacije treba redovno da vrše **stratešku analizu** kako bi stekle uvid u novonastale trendove o *modus operandiju* počinilaca, kao i kako bi bile u toku sa obrascima ponašanja korisnika tehnologije i tehnološkim okruženjem koje se brzo menja. Na osnovu ovih strateških dokaza, države tada mogu da pokrenu ciljane policijske operacije, uspostave sporazume o saradnji i osmisle ciljane kampanje za podizanje svesti. Znanje treba redovno širiti na nacionalnom i nadnacionalnom nivou.

7. Države treba da povećaju prekograničnu saradnju kroz **pojednostavljene procedure, razmenu najboljih praksi i tehnologija** (npr. specijalizovanih softvera) i pojačano **širenje praktičnih informacija** o kontakt tačkama/namenskim jedinicama koje služe kao „privilegovani kontakti" u slučaju trgovine ljudima, uključujući trgovinu ljudima posredstvom IKT. Treba podsticati saradnju i podršku između država odredišta i država porekla (npr. skupa tehnološka oprema može biti dostupna samo bogatijim državama odredišta).

## Aktivnosti za poboljšanje krivičnog gonjenja u slučajevima trgovine ljudima posredstvom tehnologije

8. Tužiocima treba obezbediti posebnu **obuku** o trgovini ljudima posredstvom tehnologije i rukovanju elektronskim dokazima, kao i izvođenju dokaza pred sudijom/porotom. Države treba da preduzmu mere kako bi osigurale da **tužioci budu upoznati sa procedura-**

**ma** za traženje elektronskih dokaza od privatnih kompanija, kao i za pribavljanje dokaza iz drugih država i saradnju sa drugim državama, kako u okviru pravnog okvira EU (preko zajedničkih istražnih timova i evropskih naloga za istragu), tako i van pravnog okvira EU.

## Aktivnosti za unapređenje saradnje sa privatnim kompanijama

9. Države bi trebale da razviju **procedure za razmenu podataka** sa kompanijama koje poseduju relevantne podatke i da razmotre razvoj **protokola za saradnju** sa privatnim kompanijama, uključujući kompanije za društvene mreže i ekonomiju honorarnih poslova, kao i platforme za iznajmljivanje kako bi se podstaklo pravovremeno pružanje informacija. Takvi protokoli/procedure treba da razjasne zakonske uslove pod kojima kompanije za IKT, ISP i pružaoci sadržaja funkcionišu; odrede kontakt tačke unutar kompanija; i razjasne koje nacionalne agencije su odgovorne za konkretne akcije, npr. traženje dokaza ili uklanjanje sadržaja povezanih sa trgovinom ljudima. Odbijanje da se podele dokazi ili uklone sadržaji povezani sa trgovinom ljudima treba da bude blagovremeno, izričito i obrazloženo.

## Aktivnosti za unapređenje međunarodne saradnje

10. Trebalo bi **uspostaviti lakši proces za zahteve za uzajamnu pravnu pomoći (UPP)**, uključujući jasnije procedure, povećanu upotrebu unapređene mreže kontaktnih tačaka, uključujući kontaktne tačke u Evropskoj pravosudnoj mreži, i omogućiti da zahtevi za uzajamnu pravnu pomoć budu jasno postavljeni i razmotreni na samom početku. Države treba da obezbede da njihovo osoblje bude adekvatno obučeno za obradu zahteva za UPP, korišćenje EIO i drugih međunarodnih alata. Države i međunarodne organizacije treba da razviju **zajednički dogovorene i prihvaćene šablone** koji podržavaju procese saradnje u cilju olakšavanja komunikacije, smanjenja administrativnih opterećenja i smanjenja broja grešaka u zahtevima. Države takođe treba da razviju upotrebu **bezbednih oblika elektronske komunikacije** i da promovišu njihovo usvajanje kako bi se olakšala međunarodna saradnja.

## Aktivnosti za unapređenje obuka

11. Trebalo bi predvideti **zajedničke aktivnosti obuke (ZAO)** za države koje se sistematski bave zajedničkim slučajevima trgovine ljudima. Transnacionalna razmena znanja može se podsticati kroz učešće u međunarodnim/regionalnim obukama koje su fokusirane na određene aspekte istraživanja trgovine ljudima posredstvom IKT. Takve obuke treba da uključuju studije slučaja i scenarije o trgovini ljudima posredstvom IKT. Za tužioce i sudije takođe treba obezbediti obuku o trgovini ljudima posredstvom IKT i o povezanim pravnim instrumentima.

12. NVO treba da prođu obuku o najnovijim dešavanjima u svetu tehnologije i u oblasti trgovine ljudima, uključujući promene u strategijama regrutovanja. NVO treba da budu u poziciji da razmenjuju iskustva o najboljim međunarodnim praksama.

## Aktivnosti za unapređenje pravnih instrumenata

13. Nadležni organi bi trebalo da osmisle **zajedničke procedure za brzu razmenu digitalnih dokaza sa ISP** i da **ponovo procene trajanje obaveza čuvanja podataka** koje su nametnute ISP (trenutni periodi su previše kratki imajući u vidu trajanje policijskih istraga). Treba uložiti napore da se usvoji **zajednički okvir** u vezi sa obavezama čuvanja podataka i razmenom elektronskih dokaza.

14. Kako bi iskoristile puni potencijal koji nudi **Konvencija o visokotehnološkom kriminalu**, države treba da (a) završe usaglašavanje nacionalnog zakonodavstva sa Konvencijom; (b) prošire i unaprede obuke o mogućnostima koje nudi Konvencija pošto trenutno ne koriste sve države ugovornice u punom potencijalu sredstva koja su im dostupna; (c) sprovode aktivnosti za podizanje svesti o širokom obimu procesnih ovlašćenja i alata za međunarodnu saradnju iz Konvencije, posebno u vezi sa predmetima trgovine ljudima; i (d) brzo sprovode mere iz Drugog dodatnog protokola.

15. Države treba pažljivo da procene pitanje gde se njihova **kontaktna tačka** (prema Konvenciji o visokotehnološkom kriminalu) nalazi u okviru sistema krivičnog pravosuđa kako bi se izbegla **uska grla**. Uz sve centralniju ulogu koju igraju IKT i elektronski dokazi, takve kontaktne tačke će biti pod sve većim pritiskom i brzo će biti preopterećene ako ne budu imale adekvatno osoblje. Države bi možda želele da razmotre popunjavanje takvih kontaktnih tačaka sa osobljem koje poseduje stručnost u različitim oblastima borbe protiv kriminala, uključujući trgovinu ljudima posredstvom IKT.

16. Države van Evrope treba ohrabriti da **usvoje ključne međunarodne pravne instrumente**, kao što su Konvencija SE o visokotehnološkom kriminalu i Konvencija SE o uzajamnom pružanju pomoći u krivičnim stvarima, kako bi se ujednačila i poboljšala međunarodna saradnja.

17. Treba povećati **saradnju i sinergiju** između mehanizma za praćenje Konvencije o borbi protiv trgovine ljudima (GRETA i Komitet ugovornica) i T-CY, na primer, u vidu razmene mišljenja, kao i razvoja aktivnosti za izgradnju kapaciteta koje se fokusiraju na obe konvencije.

## Aktivnosti za sprečavanje viktimizacije i ponovne viktimizacije

18. Privatne kompanije, u saradnji sa nadležnim organima i NVO, trebalo bi da povećaju **društveno oglašavanje** na internetu kako bi sprečile viktimizaciju i poboljšale otkrivanje trgovine ljudima posredstvom tehnologije. Države treba da povećaju svoje napore da informišu pojedince o njihovim radnim pravima na jeziku koji razumeju, u saradnji sa NVO i kompanijama koje pružaju usluge hostinga za oglase za posao. Uticaj kampanja treba rutinski procenjivati.

19. Države, NVO i privatne kompanije koje pružaju onlajn i IKT usluge treba da pokrenu inicijative za **podizanje svesti o rizicima vezanim za tehnologiju, uključujući kako trgovci ljudima mogu da iskoriste tehnologiju** i kako mogu da počnu potencijalne situacije eksploatacije. Škole i prosvetni radnici treba da budu deo ovog napora jer su deca i mladi odrasli izloženi povećanim rizicima. Države i NVO treba da rade sa privatnim kompanijama koje nude usluge komunikacije i razmene poruka kako bi u sistem ugradile informacije/upozorenja o **bezbednom korišćenju privatnih kanala komunikacije**.

20. NVO treba da ponude obuku o tehnikama zaštite podataka i bezbednoj upotrebi tehnologije u okviru **programa zaštite i reintegracije žrtava**. Žrtvama ne treba uskratiti pristup tehnologiji koji bi mogao da im oduzme moć.

## Međusektorsko delovanje

21. Države treba da dodaju tehnološku strategiju u svoje **nacionalne akcione planove** za borbu protiv trgovine ljudima.

# Prilog 1 | Izgradnja baze dokaza o trgovini ljudima posredstvom interneta i IKT: Spisak izvora

Baza dokaza je izgrađena na osnovu širokog pozadinskog istraživanja koje pokriva različite izvore, uključujući sledeće: (a) međunarodne organizacije; (b) akademske zajednice; (c) izabrane nacionalne izvestioce; (d) NVO i humanitarne organizacije; (e) privatni sektor. Ukupno 62 izvora su identifikovana kao relevantna za potrebe ovog rada. Dok razmatrani izvori obuhvataju period od 2003. do 2020. godine, velika većina je objavljena nakon 2015. godine, dok su 22 objavljena u poslednje tri godine. Svi razmatrani izvori su napisani na engleskom jeziku (sa jednim izuzetkom: francuska verzija izveštaja koji je pripremila organizacija Myria, belgijski „*Centre fédéral Migration*").

## Međunarodne i nacionalne organizacije


1. Council of Europe (2021). *Protecting Women and Girls from Violence in the Digital Age*.
2. Council of Europe (2019). *Stepping up the Council of Europe action against trafficking in human beings in the digital age*. Summary Report.
3. Council of Europe (2019). *9. opšti izveštaj o aktivnostima GRETA*.
4. Council of Europe (2016). *Safeguarding Human Rights on the Net*.
5. Council of Europe (2016). *Study on Reduction Measure to Combat Trafficking in Human Beings for the Purpose of Labour Exploitation through Engagement of the Private Sector*.
6. Council of Europe (2016). *Emerging Good Practice by State Authorities, the Business Community and Civil Society in the Area of Reducing Demand for Human Trafficking for the Purpose of Labour Exploitation*.
7. Council of Europe (2015). *Comparative study of blocking, filtering and take-down of illegal Internet content*.
8. Council of Europe (2007). *Trafficking in human beings: Internet recruitment*.
9. Council of Europe (2003). *Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation*.
10. ICAT (2019). *Human Trafficking and Technology: Trends, Challenges and Opportunities*. Inter-Agency Coordination Group Against Trafficking in Persons. Issue Brief 7.
11. OSCE (2020). *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*. OSCE and Tech Against Trafficking.
12. UN.GIFT (2008). *Technology and Human Trafficking*. The Vienna Forum to fight Human Trafficking: Background Paper.
13. UNODC (2019). Module 14: Links between Cybercrime, Trafficking in Persons and Smuggling of Migrants. E4J Teaching Modules.
14. Myria (2017). *En ligne_: Traite et trafic des êtres humains, Rapport annuel 2017*.
15. Europol (2020). *The challenges of countering human trafficking in the digital era*.
16. Europol (2014). *Trafficking in human beings and the Internet*. Intelligence Notification

## Akademska zajednica


17. Ibanez M. and Gazan R. (2016). „Detecting Sex Trafficking Circuits in the U.S. Through Analysis of Online Escort Advertisements". IEEE/ACM International Conference on Advances in Social Network Analysis and Mining (ASONAM), 892–895.

18. Ibanez M. and Gazan R. (2016). „Virtual Indicators of Sex Trafficking to Identify Potential Victims in Online Advertisements", 818–824.

19. Ibanez M. and Suthers D. D. (2014). „Detection of Domestic Human Trafficking Indicators and Movement Trends Using Content Available on Open Internet Sources". 47th Hawaii International Conference on System Science, 1556–1565.

20. Volodko A., Cockbain E. and Kleinberg B. (2019). „ 'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers". Trends in Organized Crime, 27: 7–35.

21. Di Nicola A., Baratto G. and Martini E. (2017). *Surf and Sound. The Role of the Internet in People Smuggling and Human Trafficking*. eCrime Research Report 3.

22. Sykiotou A. P. (2017). Cyber trafficking: recruiting victims of human trafficking through the net. In „Essays in Honour of Nestor Courakis". A. N. Sakkoulas Publications.

23. Foot K.A., Toft A. and Cesare N. (2015). „Developments in Anti-Trafficking Efforts: 2008 – 2011". Journal of Human Trafficking, 1:2, 136–155.

24. Gerry F., Muraszkiewicz J. and Vavoula N. (2016). „The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns". *Computer Law & Security Review*, 32:2, 205–217.

25. Latonero M., Browyn W. and Dank M. (2015). *Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study*. California: University of Southern California, Annenberg Center on Communication Leadership & Policy.

26. Latonero M. (2011). *The Role of Social Networking Sites and Online Classifieds*. California: University of Southern California, Annenberg Center on Communication Leadership & Policy Research Series.

27. Latonero M. (2012). *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*. University of Southern California, Annenberg Center on Communication Leadership & Policy.

28. Elliott J. and McCartan K., (2013). „The reality of trafficked people's access to technology". *The Journal of Criminal Law*, 77:3, pp.255–273.

29. Hughes D. M. (2014). „Trafficking in human beings in the European Union: Gender, sexual exploitation, and digital communication technologies." *Sage Open* 4: 4.

30. Kunz R., Baughman M., Yarnell R. and Williamson C. (2018). *Social Media and Sex Trafficking Process: From connection and recruitment, to sales*. Ohio: University of Toledo.

31. Farley M., Franzblau K., and Kennedy M. A. (2013). Online prostitution and trafficking. *Albany Law Review*, 77:3, 101–157.

32. Barney D. (2018). Trafficking Technology: A look at different approaches to ending technology-facilitated human trafficking. *Pepperdine Law Review*, 45, 747–784.

33. Milivojevic S., Moore H., and Segrave M. (2020). Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology. *Anti-trafficking review*, (14), 16–32

34. Raets S. and Janssens J. (2019). Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business. *European Journal on Criminal Policy and Research*, 1–24.

35. John G. (2018). Analyzing the Influence of Information and Communication Technology on the Scourge of Human Trafficking in Rwanda. Academic of Social Science Journal, 3:1, 1095–1102.

36. Maras M-H (2017). Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking?, *Journal of Internet Law*, vol. 21, 17–21.

37. Stalans L. J. and Finn M A. (2016). Understanding How the Internet Facilitates Crime and Deviance, *Victims & Offenders*, 11, 501–508.

38. Van Reisen M., Gerrima Z., Ghilazghy E., Kidane S., Rijken C., and Van Stam, G. (2017). *Tracing the emergence of ICT-enabled human trafficking for ransom*. In Piotrowicz R., Rijken C., Baerbel, Uhl B. H. (eda), The Routledge Handbook on Human Trafficking. Routledge: London

39. Raets S. and Janssens J. (2018). *Trafficking & Technology: The role of digital communication technologies in the human trafficking business*.

40. Dixon H. (2013). Human trafficking and the Internet (and other technologies, too). *Judges' Journal*, 52:1, 36–39.

41. Thakor M. and Boyd D. (2013). Networked trafficking: Reflections on technology and the anti-trafficking movement. *Dialectical Anthropology*, vol. 37, str. 277–290.

42. Michell K. J. and Boyd D. (2014). *Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law enforcement*. University of New Hampshire: Crime Against Children Research Centre.

43. Heil E. and Nichols A. (2014). Hot spot trafficking: A theoretical discussion of the potential problems associated with targeted policing and the eradication of sex trafficking in the United States. *Contemporary Justice Review*, 17(4), 421–433

44. Andrews S., Brewster B., Day T. (2016) Organised Crime and Social Media: Detecting and Corroborating Weak Signals of Human Trafficking Online. U: Haemmerlé O., Stapleton G., Faron Zucker C. (eds) Graph-Based Representation and Reasoning. ICCS 2016. *Lecture Notes in Computer Science*, vol 9717. Springer, Cham.

45. Mendel J. and Sharapov K. (2016). Human trafficking and online networks: Policy, analysis, and ignorance. *Antipode*, 48(3), 665–684

46. TRACE (2017). Report on the role of current and emerging technologies in human trafficking. Deliverable 4.1, FP7/Security Research, koje finansira Evropska komisija.

47. Landman T., Trodd Z., Darnton H., Durgana D., Moote K., Jones P., Setter C., Bliss N., Powell S. and Cockayne J. (eds). *Code 8.7: Conference Report* 2019/02/19–20 New York. New York: United Nations University, 2019.

48. Kiss L., Fotheringhame D., Mak J., McAlpine A., and Zimmerman, C. (2020). The use of Bayesian networks for realist evaluation of complex interventions: evidence for prevention of human trafficking. *Journal of Computational Social Science*, 1–24

49. Jackson B. and Lucas B. (2020). A COVID-19 Response to Modern Slavery using AI Research. 26 June, www.delta87.org

50. Rende Taylor L. and Shih E. (2019). „Worker feedback technologies and combatting modern slavery in global supply chains: examining the effectiveness of remediation–oriented and due-diligence-oriented technologies in identifying and addressing forced labour and human trafficking", *Journal of the British Academy*, 7(s1), 131–165.

51. Musto J., Thakor M., and Gerasimov B. (2020), „Editorial: Between Hope and Hype: Critical evaluations of technology's role in anti-trafficking", *Anti-Trafficking Review*, 1– 14, dostupno onlajn na: https://doi.org/10.14197/atr.201220141.

52. Kougkoulos I., Cakir M. S., Kunz N., Boyd D. S., Trautrims A., Hatzinikolaou K., and Gold S. (2021). *A multi- method approach to prioritize locations of labor exploitation for ground- based interventions*. Production and Operations Management, online first.

## NVO/humanitarne organizacije/privatni sektor

53. Fine Tune Project (2011). *The Role of the Internet in Trafficking for Labour Exploitation*. Final Report for the European Commission.

54. Thorn (2015). A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims.

55. Thorn (2018). Survivor Insights. The Role of Technology in Domestic Minor Sex Trafficking.

56. Chawki M. and Wahab M. (2005). *Technology is a double-edged sword: Illegal human trafficking in the information age*. Computer Crime Research Center.

57. Caliber (2008). *Law Enforcement Response to Human Trafficking and the Implications for Victims: Current Practices and Lessons Learned*. Final report prepared for U.S Department of Justice: National Institute of Justice.

58. Stop the Traffik (2019). Independent evaluation of Stop the Traffik's work and model.

## Veb lokacije

59. Traffik Analysis Hub: https://traffikanalysis.org/ (IBM, Stop the Traffik i Clifford Chance)

60. The Counter Trafficking Data Collaborative: https://www.ctdatacollaborative.org/ (IOM, Polaris i Liberty Shared)

61. Alan Turing Institute, Data Science for Tackling Modern Slavery: https://www.turing.ac.uk/research/research-projects/data-science-tackling-modern-slavery

62. UN Delta 8.7. Alliance 8.7 Knowledge Problem: https://delta87.org/ (Globalna platforma za razmenu znanja koja istražuje šta doprinosi eliminaciji prinudnog rada, modernog ropstva, trgovine ljudima i dečijeg rada, Cilj 8.7 predviđen Ciljevima održivog razvoja UN)

# Prilog 2. | Upitnik za državne aktere

## Deo 1. Uticaj IKT na trgovinu ljudima

1. Na osnovu dokaza do kojih se došlo u vašoj zemlji, da li možete da navedete primere kako počinioci koriste IKT u kontekstu trgovine ljudima u svrhu seksualne eksploatacije? (Za svaki primer navedite detalje o načinu rada trgovaca ljudima i o vrsti korišćene tehnologije, npr. internet, određene veb lokacije, društveni mediji, aplikacije).

2. Slično tome, da li možete da navedete primere kako počinioci koriste IKT u kontekstu trgovine ljudima u svrhu radne eksploatacije? (Za svaki primer navedite detalje o načinu rada trgovaca ljudima i o vrsti korišćene tehnologije, npr. internet, određene veb lokacije, društveni mediji, aplikacije *i* privredni sektor u kojem se eksploatacija odvija).

3. Koji su novi trendovi u vašoj državi u vezi sa upotrebom IKT u trgovini ljudima (nove vrste tehnologije, novi modus operandi, nove vrste eksploatacije...)? Da li ste identifikovali nove prakse na internetu koje mogu da povećaju rizik da neko postane žrtva trgovine ljudima (i u svrhu seksualne i u svrhu radne eksploatacije)?

4. Da li mračna mreža igra bilo kakvu ulogu u trgovini ljudima u vašoj državi? Ako igra, možete li da navedete neke detalje? (Pod mračnom mrežom se podrazumevaju internet stranice koje su dostupne samo preko anonimizujućih pregledača, kao što je Tor).

5. Da li se u vašoj državi IKT koriste za omogućavanje finansijskih tokova u kontekstu trgovine ljudima? Ako da, na koje načine? U kojoj meri se koriste kriptovalute ili kripto novčanici?

6. Uopšteno, na skali od 1 do 5, kako biste ocenili uticaj IKT na trgovinu ljudima u vašoj državi?

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Veoma ograničen | | | | Veoma značajan |

## Deo 2. Ključni izazovi sa kojima se suočavaju države ugovornice prilikom otkrivanja, istraživanja i krivičnog gonjenja trgovine ljudima posredstvom IKT

Otkrivanje

7. Koje su strategije usvojene u vašoj državi za otkrivanje slučajeva trgovine ljudima na internetu?

8. Uopšteno govoreći, koji su izazovi u otkrivanju trgovine ljudima posredstvom IKT?

9. Da li možete da navedete neke primere najboljih praksi u otkrivanju slučajeva trgovine ljudima posredstvom IKT?

10. Koju vrstu obuke pružate za istražitelje i druge aktere iz sistema krivičnog pravosuđa u pogledu identifikacije slučajeva trgovine ljudima posredstvom IKT? Koja dodatna obuka bi se mogla organizovati kako bi se povećala efikasnost strategija otkrivanja? Kako bi se mogla ojačati onlajn identifikacija žrtava?

Istrage

11. Kada je reč o **istragama trgovine ljudima posredstvom IKT**, koliki problem predstavlja sledeće:

| | Obično nije problem | Mali problem | Veliki problem |
|---|---|---|---|
| Šifrovanje podataka | | | |
| Nedostatak tehničkog znanja među organima za sprovođenje zakona | | | |
| Velika količina podataka dovodi do istraga za koje je potrebno mnogo vremena | | | |
| Brzina tehnoloških promena (nove tehnologije se brzo pojavljuju itd.) | | | |
| Nedostatak tehničke opreme | | | |
| Nedostatak pomoći privatnog sektora | | | |
| Neodgovarajući zakonodavni instrumenti, uključujući instrumente za uzajamnu pravnu pomoć | | | |

12. Za svaki problem koji smatrate „velikim", navedite nekoliko primera i opišite korake, ako postoje, koji su već preduzeti kako biste ih prevazišli/ublažili. Za svaki „veliki" problem, koja rešenja bi se mogla predvideti za njegovo prevazilaženje?

13. Da li postoje dodatni problemi koji nisu navedeni u tabeli? (Za svaki dodatni problem, navedite detalje o problemu i rešenjima koja bi se mogla predvideti za njegovo prevazilaženje).

14. Koje su po vašem mišljenju najbolje strategije za vođenje delotvornih istraga trgovine ljudima posredstvom IKT?

15. Koje obuke se trenutno organizuju za organe za sprovođenje zakona u vezi sa istragama trgovine ljudima posredstvom IKT? Koje dodatne potrebe za obukama za organe za sprovođenje zakona ste identifikovali u vezi sa trgovinom ljudima posredstvom IKT? Da li postoje primeri praksi pri sprovođenju obuka koje smatrate posebno uspešnim?

## Krivično gonjenje

16. Kada je reč o **krivičnom gonjenju trgovine ljudima posredstvom IKT**, koliki problem predstavlja sledeće:

| | Obično nije problem | Mali problem | Veliki problem |
|---|---|---|---|
| Određivanje nadležnosti | | | |
| Ekstradicija osumnjičenih | | | |
| Pribavljanje dokaza iz drugih država | | | |
| Pomoć privatnog sektora | | | |
| Neodgovarajući zakonodavni instrumenti, uključujući instrumente za uzajamnu pravnu pomoć | | | |
| Nedovoljna obuka tužilaca | | | |

17. Za svaki problem koji smatrate „velikim", navedite nekoliko primera i opišite korake, ako postoje, koji su već preduzeti kako biste ih prevazišli/ublažili. Za svaki „veliki" problem, koja rešenja bi se mogla predvideti za njegovo prevazilaženje?
18. Da li postoje dodatni problemi koji nisu navedeni u tabeli? (Za svaki dodatni problem, navedite detalje o problemu i rešenjima koja bi se mogla predvideti za njegovo prevazilaženje).
19. Koje obuke se trenutno organizuju za tužioce i sudije u vezi sa istragama trgovine ljudima posredstvom IKT? Koje dodatne potrebe za obukama za tužioce i sudije ste identifikovali u vezi sa trgovinom ljudima posredstvom IKT? Da li postoje primeri praksi pri sprovođenju obuka koje smatrate posebno uspešnim?
20. Da li u vašoj državi postoje specijalizovane jedinice u okviru organa za sprovođenje zakona i pravosuđa čiji zadatak je vođenje predmeta trgovine ljudima sa bitnom tehnološkom komponentom (npr. elektronski i onlajn dokazi)? Ako je odgovor da, opišite njihove prakse.

## Međunarodna saradnja

21. Koji izazovi se sreću tokom transnacionalnih istraga i pravosudne saradnje u kontekstu trgovine ljudima posredstvom IKT? Koje su najveće prepreke za delotvornost, ako postoje, i kako se one prevazilaze?
22. Koji su primeri dobrih praksi za unapređenje međunarodne saradnje?

## Deo 3. Postojeći alati koji doprinose sprečavanju i borbi protiv trgovine ljudima posredstvom IKT

23. Da li možete da opišete najznačajnije nacionalne pravne instrumente koji se koriste u borbi protiv trgovine ljudima posredstvom IKT? Da li vaše zakonodavstvo uspeva da prati korak sa tehnološkim promenama? Ako je odgovor da, kako se prilagođavate takvim promenama? Ako je odgovor ne, kako se situacija može unaprediti?

24. Da li možete da opišete najznačajnije međunarodne pravne instrumente koji se koriste u borbi protiv trgovine ljudima posredstvom IKT? Da li smatrate da su postojeći instrumenti adekvatni? Na koji način bi se mogli unaprediti?

25. Da li postoje određeni nedostaci u postojećem nacionalnom ili međunarodnom zakonodavstvu koji ometaju borbu protiv trgovine ljudima posredstvom IKT?

26. Da li imate mehanizme usmereni na sprečavanje upotrebe IKT u svrhu trgovine ljudima, uključujući na društvenim medijima i u vezi sa oglasima za posao na internetu? Ako imate, opišite postojeće prakse i navedite koji državni organ je odgovoran za njihovo sprovođenje.

## Deo 4. Korišćenje tehnologije

27. Koji tehnološki alati, ako postoje, su trenutno dostupni u vašoj državi za identifikaciju žrtava trgovine ljudima? Da li se za identifikaciju žrtava koristi veštačka inteligencija, tehnologija za prepoznavanje lica i/ili analiza velikih količina podataka? Da li imate skup indikatora („znakova upozorenja") za identifikaciju žrtava?

28. Koje inicijative zasnovane na tehnologiji postoje u vašoj državi za pomoć žrtvama i širenje informacija među ugroženim zajednicama?

29. Koje inicijative zasnovane na tehnologiji postoje u vašoj državi za pomoć istragama i unapređenje krivičnog gonjenja?

## Deo 5. Saradnja sa privatnim kompanijama

30. Na koje načine kompanije za IKT, uključujući pružaoce usluga hostovanja interneta, društvenih medija i drugih onlajn platformi, pomažu pri identifikaciji i uklanjanju internet sadržaja povezanih sa trgovinom ljudima? Kako se vrši filtriranje? Da li su aktuelni mehanizmi za filtriranje i uklanjanje delotvorni? Ako nisu, kako bi se mogli poboljšati? Da li možete da navedete primere dobrih praksi?

31. Da li postoje zahtevi u vašem pravnom okviru za filtriranje i uklanjanje internet sadržaja povezanih sa trgovinom ljudima i koje sankcije su predviđene za nepoštovanje takvih zahteva? Da li postoji kodeks ponašanja za pružaoce usluga/sadržaja? Da li je pravni okvir delotvoran? Ako nije, kako bi se mogao poboljšati?

32. Koje su prepreke sa kojima se suočava vaša država pri radu sa kompanijama za IKT i pružaocima internet usluga, uključujući pružaoce sadržaja i društvene medije, tokom borbe protiv trgovine ljudima? Kako se može razviti efikasno partnerstvo sa kompanijama za IKT? Koji alati – pravni i operativni – bi mogli ojačati saradnju sa kompanijama za IKT?

33. Na koje načine se kompanije za IKT bore protiv finansijskih transakcija povezanih sa trgovinom ljudima? Kako bi se saradnja u ovom pogledu mogla ojačati?

34. Da li u vašoj državi postoji nezavisno telo/regulator zadužen za praćenje internet sadržaja? Ako postoji, na kojoj osnovi se takve aktivnosti sprovode? Ako ne postoji, na koji način se vrši praćenje?

## Deo 6. Konvencija o visokotehnološkom kriminalu (Budimpeštanska konvencija)

35. Na koje načine, ako je to slučaj, vaša država koristi odredbe Konvencije SE o visokotehnološkom kriminalu (Budimpeštanske konvencije) za borbu protiv trgovine ljudima? Ako ne koristi, zašto je to tako?

36. Da li postoje načini kako bi se Konvencija o visokotehnološkom kriminalu (Budimpeštanska konvencija) i njeni dodatni protokoli mogli dodatno koristiti za borbu protiv trgovine ljudima?

## Deo 7. Zaštita ljudskih prava

37. Koje mere postoje za zaštitu ljudskih i građanskih prava pojedinaca, uključujući prava na zaštitu podataka i privatnosti, u kontekstu borbe protiv trgovine ljudima posredstvom IKT? Ako se koriste tehnološki alati, na primer, detaljno pregledanje interneta, koji protokoli postoje kako bi se obezbedilo da takvi alati štite osetljive podatke, uključujući podatke o seksualnoj orijentaciji, veroispovesti i političkim stavovima?

38. Da li imate rodno osetljive protokole povezane sa upotrebom tehnologije u borbi protiv trgovine ljudima? Da li imate starosno osetljive protokole? Ako imate, možete li da opišete ove protokole?

39. Kako se čuva poverljivost podataka pri deljenju informacija sa organima za sprovođenje zakona i trećim licima, uključujući privatne kompanije i humanitarne organizacije? Kako je uspostavljena ravnoteža između potrebe žrtava za poverljivošću prilikom korišćenja usluga i potrebe za prikupljanjem dokaza i informacija za borbu protiv trgovine ljudima?

**Na kraju, da li postoji još nešto što nije navedeno u ovom upitniku, a što smatrate relevantnim u kontekstu borbe protiv trgovine ljudima posredstvom IKT?**

## Dodatni materijali

Da li možete da navedete bilo koje relevantne materijale koji nisu poverljive prirode, uključujući statističke podatke, saopštenja za medije, sažetke policijskih operacija, koji se odnose na trgovinu ljudima posredstvom IKT, uključujući sledeće:

- Upotreba IKT u trgovini ljudima;
- Izazovi u otkrivanju trgovine ljudima posredstvom IKT, uključujući identifikaciju žrtava;
- Izazovi koji se sreću tokom istraživanja i krivičnog gonjenja trgovine ljudima posredstvom IKT;
- Prekogranična saradnja u kontekstu trgovine ljudima posredstvom IKT;
- Saradnja sa kompanijama za IKT;
- Alati za borbu protiv trgovine ljudima posredstvom IKT (pravni i/ili operativni alati)
- Inicijative zasnovane na tehnologiji za borbu protiv trgovine ljudima;
- Primeri dobrih praksi

Ako je vaš nacionalni izvestilac istražio pitanje trgovine ljudima posredstvom IKT, podelite sa nama relevantne izveštaje/materijale.

# Prilog 3. | Upitnik za NVO

Svrha ovog upitnika je da se shvati uticaj tehnologije na trgovinu ljudima na osnovu dokaza prikupljenih tokom rada na terenu. Termin „tehnologija" ovde podrazumeva širok skup informacionih i komunikacionih tehnologija (IKT) koje korisnicima omogućavaju razmenu digitalnih informacija. Primeri tehnologija uključuju internet, onlajn društvene medije i aplikacije za mobilne telefone.

## Deo 1. Uticaj tehnologije na trgovinu ljudima

1. Na osnovu dokaza do kojih se došlo u vašem radu, da li možete da navedete primere kako počinioci koriste tehnologiju (IKT) u kontekstu trgovine ljudima u svrhu seksualne, radne ili druge vrste eksploatacije? (Za svaki primer navedite detalje o vrsti eksploatacije i vrsti korišćene tehnologije, npr. internet, određene veb lokacije, društveni mediji, aplikacije).
2. Da li ste identifikovali nove prakse na internetu koje mogu da povećaju rizik da neko postane žrtva trgovine ljudima?
3. Koji su izazovi u otkrivanju trgovine ljudima posredstvom tehnologije? Kako bi se mogla ojačati identifikacija žrtava?
4. Da li možete da navedete neke primere dobrih praksi koje ste razvili za otkrivanje slučajeva trgovine ljudima posredstvom tehnologije i za identifikaciju žrtava?
5. Da li sarađujete sa agencijama za sprovođenje zakona u borbi protiv trgovine ljudima posredstvom tehnologije? Koje su prepreke takvoj saradnji i kako bi se mogle prevazići?
6. Kakve obuke, ako postoje, organizujete za svoje osoblje i volontere u vezi sa uticajem tehnologije na trgovinu ljudima? Koja dodatna obuka bi bila korisna za povećanje efikasnosti strategija otkrivanja? Da li imate tim u vašoj organizaciji koji je specijalizovan za trgovinu ljudima posredstvom tehnologije?
7. Da li postoje određeni nedostaci u postojećem nacionalnom ili međunarodnom zakonodavstvu koji ometaju borbu protiv trgovine ljudima posredstvom tehnologije?

## Deo 2. Korišćenje tehnologije za borbu protiv trgovine ljudima

8. Koji tehnološki alati, ako postoje, su trenutno dostupni kao pomoćno sredstvo za identifikaciju žrtava trgovine ljudima (npr. određene aplikacije, analiza velikih količina podataka, skeniranje interneta)? Da li imate skup indikatora („znakova upozorenja") za identifikaciju potencijalnih žrtava? Koju vrstu tehnoloških alata bi moglo biti korisno imati?
9. Koje inicijative zasnovane na tehnologiji, ako postoje, su vam na raspolaganju za pomoć žrtvama i širenje informacija među ugroženim zajednicama? Koje inicijative zasnovane na tehnologiji bi bilo korisno razviti?
10. Da li ste organizovali kampanje za podizanje svesti usmerene na korišćenje tehnologije u trgovini ljudima? Ako jeste, možete li da navedete neke od detalja o takvim kampanjama?
11. Da li imate rodno osetljive protokole povezane sa upotrebom tehnologije u borbi protiv trgovine ljudima? Da li imate starosno osetljive protokole? Ako imate, možete li da opišete ove protokole?
12. Kako se čuva poverljivost podataka pri deljenju informacija sa organima za sprovođenje zakona? Kako je uspostavljena ravnoteža između potrebe žrtava za poverljivošću prilikom korišćenja usluga i potrebe za prikupljanjem dokaza za borbu protiv trgovine ljudima?

13. Na osnovu dokaza prikupljenih u vašem radu, kako biste ocenili uticaj tehnologije na trgovinu ljudima na skali od 1 do 5?

| **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|
| Veoma ograničen | | | | Veoma značajan |

**Na kraju, da li postoji još nešto što nije navedeno u ovom upitniku, a što smatrate relevantnim u kontekstu borbe protiv trgovine ljudima posredstvom IKT?**

## Dodatni materijali

Ako je to moguće, da li možete da podelite s nama bilo koje relevantne materijale koje ste izradili, uključujući statističke podatke, saopštenja za medije i izveštaje, a koji se odnose na trgovinu ljudima posredstvom tehnologije.

# Prilog 4. | Upitnik za tehnološke kompanije

Svrha ovog upitnika je da se shvati uticaj tehnologije na trgovinu ljudima na osnovu dokaza prikupljenih tokom rada na terenu. Termin „tehnologija" ovde podrazumeva širok skup informacionih i komunikacionih tehnologija (IKT) koje korisnicima omogućavaju razmenu digitalnih informacija. Primeri tehnologija uključuju internet, onlajn društvene medije i aplikacije za mobilne telefone.

## Deo 1. Uticaj IKT na trgovinu ljudima

1. Na osnovu dokaza kojima raspolaže vaša kompanija/sektor, da li možete da opišete načine kako počinioci zloupotrebljavaju IKT u kontekstu trgovine ljudima (u svrhu seksualne, radne ili druge vrste eksploatacije)?
2. Da li ste identifikovali nove prakse na internetu koje mogu da povećaju rizik da neko postane žrtva trgovine ljudima?
3. Koji mehanizmi su razvijeni u vašoj kompaniji, ili uopšteno u vašem sektoru, za sprečavanje zloupotrebe IKT u svrhu trgovine ljudima?

## Deo 2. Saradnja sa agencijama za sprovođenje zakona i civilnim društvom

4. Na koje načine, ako je to slučaj, vaša kompanija sarađuje sa agencijama za sprovođenje zakona kako bi se omogućile identifikacija žrtava i istrage u predmetima trgovine ljudima posredstvom IKT?
5. Koje su najvažnije prepreke koje se sreću tokom saradnje sa agencijama za sprovođenje zakona u kontekstu trgovine ljudima posredstvom IKT?
6. Da li postoje primeri dobrih praksi za unapređenje saradnje sa agencijama za sprovođenje zakona?
7. Koje pravne zahteve vaša kompanija mora da poštuje u kontekstu borbe protiv trgovine ljudima?
8. Koji alati – pravni i operativni – bi mogli ojačati saradnju sa agencijama za sprovođenje zakona?
9. Na koje načine, ako je to slučaj, vaša kompanija sarađuje sa civilnim društvom kako bi se omogućila identifikacija žrtava i pomoć žrtvama trgovine ljudima?

## Deo 3. Korišćenje tehnologije

10. Koji tehnološki alati, ako postoje, su trenutno dostupni vašoj kompaniji za identifikaciju žrtava trgovine ljudima? Da li se za identifikaciju žrtava koristi veštačka inteligencija, tehnologija za prepoznavanje lica i/ili analiza velikih količina podataka? Da li imate skup indikatora („znakova upozorenja")?
11. Koje inicijative zasnovane na tehnologiji postoje u vašem sektoru za pomoć istragama i unapređenje krivičnog gonjenja?
12. Koje mere postoje za zaštitu ljudskih i građanskih prava pojedinaca, uključujući prava na zaštitu podataka i privatnosti, u kontekstu borbe protiv trgovine ljudima posredstvom IKT? Ako se koriste tehnološki alati, na primer, detaljno pregledanje interneta, koji protokoli postoje kako bi se obezbedilo da takvi alati štite osetljive podatke, uključujući po-

datke o seksualnoj orijentaciji, veroispovesti i političkim stavovima? Da li imate starosno osetljive protokole?

13. Kakve obuke, ako postoje, organizujete za svoje osoblje u vezi sa uticajem tehnologije na trgovinu ljudima? Koja dodatna obuka bi mogla povećati efikasnost strategija za borbu protiv trgovine ljudima?

**Na kraju, da li postoji još nešto što nije navedeno u ovom upitniku, a što smatrate relevantnim u kontekstu borbe protiv trgovine ljudima posredstvom IKT?**

## Dodatni materijali

Ako je to moguće, podelite s nama bilo koje relevantne materijale koji nisu poverljive prirode, uključujući statističke podatke, saopštenja za medije i izveštaje, a koji se odnose na trgovinu ljudima posredstvom tehnologije.

*Prevod ovog dokumenta je pripremljen uz finansijsku podršku Evropske unije i Saveta Evrope. Sadržaj je isključiva odgovornost autora i ni u kom slučaju ne predstavlja zvanične stavove Evropske unije ni Saveta Evrope.*

SRP

Zemlje članice Evropske unije su odlučile da udruže svoja znanja, resurse i sudbine. Zajedno su izgradile stabilno okruženje, demokratiju i održivi razvoj zadržavajući kulturnu raznolikost, toleranciju i individualne slobode. Evropska unija je posvećena deljenju svojih dostignuća i vrednosti sa zemljama i narodima van svojih granica.

**www.europa.eu**

Savet Evrope je vodeća organizacija za ljudska prava na kontinentu. Obuhvata 46 država, uključujući sve članice Evropske unije. Sve države članice Saveta Evrope potpisale su Evropsku konvenciju o ljudskim pravima, sporazum čiji je cilj zaštita ljudskih prava, demokratije i vladavine prava. Evropski sud za ljudska prava nadgleda primenu Konvencije u državama članicama.

**www.coe.int**

Prevod sufinansirala Evropska unija

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE